



Silver Jubilee Celebration • 25 Years of Excellence



3rd International Conference on Emerging Trends: Innovations & Challenges in Information Technology and Management

10th and 11th April 2026

Organized by

Bharati Vidyapeeth's
Institute of Management & Information Technology,
Navi-Mumbai



ABOUT BHARATI VIDYAPEETH & ABOUT INSTITUTE :

Founded in 1964 by Dr. Patangrao Kadam, Bharati Vidyapeeth embodies the vision of "Social Transformation through Dynamic Education." With 169 institutions across India, it promotes excellence in education from pre-primary to postgraduate levels. Established in 2002, BVIMIT continues this legacy by fostering innovation, industry interaction, and IT skills that prepare students to excel in the modern technological world.

ABOUT ICET 2026 :

International Conference on Emerging Trends: Innovation & Challenges in Information Technology and Management 2026, organized by Bharati Vidyapeeth's Institute of Management and Information Technology (BVIMIT), Navi Mumbai, aims to promote research and innovation in Computer Applications, Computer Science, and Management. The conference focuses on emerging technologies, trends, and challenges shaping diverse domains and services. It provides a platform for academicians, researchers, and industry professionals to exchange ideas, share advancements, and foster collaboration between theory and practice.

CHIEF PATRON :

Hon'ble Dr. Shivajirao Kadam,
Chancellor Bharati Vidyapeeth (Deemed
to be University), Pune

Hon'ble Dr. Vivek Saoji,
Vice Chancellor, Bharati Vidyapeeth
(Deemed to be University), Pune

Hon'ble Dr. Vishwajeet Kadam,
Pro-Vice Chancellor and Secretary
Bharati Vidyapeeth, (Deemed to be University), Pune.

PATRON :

Dr. V. J. Kadam,
Director, Educational Complex, Navi
Mumbai

GENERAL CHAIR :

Dr. Suhasini Vijaykumar,
Principal BVIMIT, Navi Mumbai



CONVENER :

Dr. Shambhu Shankar Rai,
Assistant Professor

Dr. Nidhi,
Assistant Professor

CO-CONVENER :

Dr. Rasika Patil,
Assistant Professor

CHIEF EDITORS :

Dr. Suhasini Vijaykumar,
Principal BVIMIT, Navi Mumbai.

Dr. Jyoti Kharade,
Associate Professor, BVIMIT

Dr. Shambhu Shankar Rai,
Assistant Professor

Dr. Nidhi Poonia,
Assistant Professor

Dr. Rasika Patil,
Assistant Professor

EDITORS :

Dr. Priya Chandran,
Associate Professor, BVIMIT

Dr. Pratibha Deshmukh ,
Associate Professor, BVIMIT

Ms. Shravani Pawar,
Assistant Professor, BVIMIT

Ms. Shubhangi Mahadik,
Assistant Professor, BVIMIT

Mrs. Sudeshna Roy,
Assistant Professor, BVIMIT

Mr. Manish Kumar,
Assistant Professor, BVIMIT

ADVISORY COMMITTEE :

Siddhartho Sengupta, Director, AWS Business Unit (Sales and GTM Strategy Head – Financial Services and Insurance for North America) at TCS

Mr. Gaurav Goel, Head of IT, Tele2 AB, Stockholm, Sweden

Dr. Durgesh Kumar Mishra, Director, SCSIT, Symbiosis, Indore

Dr. Krishan Tuli, HOD University Institute of Computing, Chandigarh University, Punjab

Dr. Gopakumaran Thampi, Principal, TSEC, University of Mumbai

Dr. Sachin Kadam, Professor, Head – Ph.D. Section, Bharati Vidyapeeth University, Pune

Dr. Bindu Krishnan, Senior Statistician, Data & AI, IBM India Software Labs, Kochi, Kerala

Dr. Rajeev R R, Programme Head, ICFOSS, Kerala

Dr. Narendra M. Shekokar, HOD CS, D.J. Sanghvi College of Engineering, Mumbai

Dr. Ganesh Magar, HOD, PG Dept. of CS, SNTD University

ORGANIZING COMMITTEE :

Dr. Jyoti Kharade, Associate Professor, BVIMIT

Ms. Shravani Pawar, Assistant Professor, BVIMIT

Ms. Shubhangi Mahadik, Assistant Professor, BVIMIT

Dr. Pratibha Deshmukh , Assistant Professor, BVIMIT

Dr. Priya Chandran, Assistant Professor, BVIMIT

Mrs. Sudeshna Roy, Assistant Professor, BVIMIT

Mr. Manish Kumar, Assistant Professor, BVIMIT

Conference Proceedings

ICET 2026

3rd International Conference on
Emerging Trends: Innovations &
Challenges in Information
Technology and Management

10th and 11th April, 2026

Organized By

Bharati Vidyapeeth's Institute of
Management and Information
Technology, Navi Mumbai
(NBA Accredited, Affiliated to University
of Mumbai)

3rd International Conference on Emerging Trends: Innovations & Challenges in Information Technology and Management



India | Australia
www.bharatglobalpublications.com
info@bharatglobalpublications.com

3rd International Conference on Emerging Trends: Innovations & Challenges in Information Technology and Management

Editors By:

Dr. Suhasini Vijaykumar

Professor of Computer Science & Approved Ph.D. Guide
University of Mumbai, Mumbai, India

Dr. Jyoti Kharade

Vice Principal & Associate Professor
Bharati Vidyapeeth's Institute of Management & Information Technology,
Navi Mumbai

Dr. Shambhu Rai

Assistant Professor
Bharati Vidyapeeth Institute of Management and Information Technology,
Navi Mumbai, India

Dr. Nidhi

Assistant Professor
Bharati Vidyapeeth Institute of Management and Information Technology,
Navi Mumbai, India

Copyright 2026 by Dr. Suhasini Vijaykumar, Dr. Jyoti Kharade, Dr. Shambhu Rai and Dr. Nidhi

First Impression: April 2026

**3rd International Conference on Emerging
Trends: Innovations & Challenges in
Information Technology and Management**

ISBN: 978-93-49554-13-9

DOI: <https://doi.org/10.5281/zenodo.20171194>

Rs. 699/- (\$80)

No part of the book may be printed, copied, stored, retrieved, duplicated and reproduced in any form without the written permission of the editor/publisher.

DISCLAIMER

Information contained in this book has been published by Bharat Global Publications and has been obtained by the Authors from sources believed to be reliable and correct to the best of their knowledge. The authors are solely responsible for the contents of the articles compiled in this book. Responsibility of authenticity of the work or the concepts/views presented by the author through this book shall lie with the author and the publisher has no role or claim or any responsibility in this regard. Errors, if any, are purely unintentional and readers are requested to communicate such error to the author to avoid discrepancies in future.

Published by:



**Bharat
Global
Publications**

Preface

Recent trends in Information Technology and Management are prominently reflected in the Proceedings of the 3rd International Conference on Emerging Trends: Innovations & Challenges in Information Technology and Management (ICET 2026), held on 10th and 11th April 2026 in hybrid mode. This volume presents a carefully selected collection of peer-reviewed research papers, highlighting contemporary developments and innovations. The editors trust that this publication will serve as a valuable resource for researchers and practitioners.

The overwhelming response to ICET 2026 is reflected in the large number of research papers received from across the country. After a rigorous peer-review and screening process, a selected number of high-quality papers have been included in this proceedings volume. These contributions represent diverse and contemporary research areas, highlighting innovative approaches, emerging technologies, and practical solutions to current challenges.

The objective of this conference has been to foster collaboration between academia and industry, encourage interdisciplinary research, and provide a forum for intellectual exchange. The selected papers not only demonstrate academic rigor but also offer insights that can contribute to real-world applications and future research directions.

We would like to express our sincere gratitude to all authors for their valuable contributions, the reviewers for their meticulous evaluation, and the organizing committee for their dedicated efforts in making this conference a success. We are also thankful to our distinguished speakers and guests for enriching the event with their knowledge and experience.

It is my earnest hope that the proceedings will serve as a valuable resource for researchers, practitioners, and students, inspiring further research and innovation in the dynamic domains of Information Technology and Management.

Dr. Suhasini Vijaykumar
Dr. Jyoti kharade
Dr. Shambhu Rai
Dr. Nidhi

Conference Coordinators/ Editors ICET 2026
BVIMIT, CBD Belapur

Acknowledgement

The publication of the Proceedings of the 3rd International Conference on Emerging Trends: Innovations & Challenges in Information Technology and Management (ICET 2026) has been made possible through the invaluable guidance, support, and collective efforts of numerous distinguished individuals.

We express our deepest gratitude to the Hon'ble Chief Patrons, Dr. Shivajirao Kadam, Chancellor, Bharati Vidyapeeth, Dr. Vishwajeet Kadam, Secretary and Pro-Vice Chancellor, Bharati Vidyapeeth Pune, and Dr. Vivek Saoji, Vice Chancellor, Bharati Vidyapeeth Pune, for their visionary leadership and continuous encouragement. We are equally thankful to our Patron, Dr. V. J. Kadam, Director, Educational Complex, Navi Mumbai, for his constant support and motivation.

We are deeply indebted to our distinguished Chief Guest, Dr. Sachin Kadam, Professor of Computer Applications, Head Ph.D Section, Director ICT Bharati Vidyapeeth Pune, Guest of Honour, Shri Ashish Mohan Jha Cofounder and COO Impactsure and Session Chair Dr. Swati Vitkar, Principal SK College of Science and Commerce Nerul. for their valuable insights and for gracing the conference with their presence. Their contributions added great value to the academic and professional discussions.

We are highly grateful to the members of the Advisory Committee for their expert guidance and valuable suggestions, which significantly enhanced the quality and impact of the conference. We extend our heartfelt thanks to all the authors who submitted their research papers and contributed to the richness of this proceedings volume. We also acknowledge the contributions of the Organizing Committee members and technical committee for their tireless efforts and commitment in ensuring the smooth conduct of the conference.

Finally, we thank the publisher for their cooperation and support in bringing out this proceedings book in a timely and professional manner. We sincerely hope that this volume will serve as a valuable reference for researchers, academicians, and practitioners in the field.

Dr. Suhasini Vijaykumar

Dr. Jyoti kharade

Dr. Shambhu Rai

Dr. Nidhi

V

About the Editors



Dr. Suhasini Vijaykumar is a distinguished academician with a Ph.D. in Computer Science from SNDT Women's University, Mumbai, and over two decades of experience in teaching and research. Her areas of specialization include Artificial Intelligence, Machine Learning, Data Mining, Internet of Things, Cybersecurity, Computer Networks, and Advanced Databases. She is an approved Ph.D. guide at the University of Mumbai and holds patents in AI-enabled intelligent systems and smart diagnostic devices. With numerous publications in Scopus and Web of Science indexed journals, she serves as a reviewer for reputed international journals and conferences. Dr. Suhasini is also a member of Boards of Studies for Computer Science and MCA programs under the University of Mumbai.



Dr. Jyoti Kharade has completed M.C.A, M.Phil. & received Ph.D. from SNDT University. She has 23 years of Experience in teaching and research. She was Board Of Studies (BOS) Member Computer Applications University of Mumbai, MSC IT, Ruai College. She has won Second prize at National level Educational Games EG 100 Challenge organized by CDAC & IEEE Bombay section in 2021. She has won Gold medal for AIMS-WeSchool Innovation Award in 2012 and 2014. She has published around 21 research papers in International Journals and Conferences. She has conducted Various FDP, Seminars, and workshops in various Institutes. She has received minor research grants and consultancy grants.



Dr Shambhu Shankar Rai working as assistant Professor at BVIMIT Navi Mumbai. 18+ years of experience in teaching for BCA and MCA students. Published more than 34 papers in reputed national and International journals. Published 4 books and one patent. Area of interest is Machine Learning and Artificial Intelligence, Computer Network, Network Security, NLP and Operating system.



Dr. Nidhi is an academician serving as an Assistant Professor in the MCA Department at BVIMIT, Navi Mumbai. She holds Ph.D. in Computer Applications with specialization in Information Security Domain. With over 15 years of teaching experience, she has contributed significantly to academia through research, curriculum development, reviewer, editor board member etc. She has published more than 30 research papers. Her expertise includes Cyber Security, DAA, Distributed Systems, Cloud Computing, Computer Network, Advanced java.

Table of Contents

COMPARATIVE EVALUATION OF MACHINE LEARNING AND ENSEMBLE MODELS FOR EARLY DETECTION OF POLYCYSTIC OVARY SYNDROME (PCOS)	1 – 11
<i>Shreya Gupta, Shreya Bhandari, Smridhi Katyal, Khyati Alhawati, Sakshi and Jagriti Singh</i>	
ML POWERED STUDENT PERFORMANCE ANALYSIS SYSTEM	12 – 24
<i>Dr. Shambhu Shankar Rai, Priyanka Dharade and Darshan Hodage</i>	
COGNITIVE LOAD BASED UI PERSONALIZATION ENGINE	25 – 34
<i>Gandhar Bagde, Janhvi Dhale, Ibrahim Khan and Sejal Vartak</i>	
GENERATIVE ADVERSARIAL NETWORKS AND EXPLAINABLE AI IN RADIOLOGY: A NOVEL FRAMEWORK FOR ENHANCED IMAGING AND DIAGNOSIS	35 – 47
<i>Mokara Praneetha, Raikindi Sravan Kumar, Mamta Narwaria and Renu Mishra</i>	
SKIN DISEASE DETECTION USING DEEP LEARNING: A COMPREHENSIVE ANALYSIS	48 – 56
<i>Ansh Dullat, Arnav Sharma, Arpit Kumar Arya and Sameer Yadav</i>	
A COMPREHENSIVE REVIEW OF AN AUTONOMOUS, EXPLAINABLE, AND MULTI-DISEASE CLINICAL RISK PREDICTION & DECISION SUPPORT	57 – 64
<i>Rudra Tyagi, Paras Tomar, Divyanshi Goel and Sarthak Agarwal</i>	

CARDIO CARE ANALYZER: AN INTELLIGENT MACHINE LEARNING FRAMEWORK FOR EARLY CARDIOVASCULAR DISEASE RISK DETECTION AND ASSESSMENT	65 – 76
<i>Siddhika Bhimrao Belsare and Prof. Shubhangi Mahadik</i>	
AI-BASED MEDICAL REPORT ANALYSIS SYSTEM USING NLP AND MACHINE LEARNING	78 - 89
<i>Aanchal Rana, Anshika Sharma and Abhinav Tyagi</i>	
SHAP-DRIVEN DEMAND FORECASTING: AN EXPLAINABLE TEMPORAL FUSION TRANSFORMER FRAMEWORK FOR INVENTORY OPTIMIZATION	90 – 99
<i>Dr. Jyoti Kharade, Sujal Baraskar, Abhishek Singh and Vaibhav Janaskar</i>	
LIVE POT HOLE DETECTION SYSTEM USING DEEP LEARNING	100 - 110
<i>Dr. Priya Chandran, Tanuja Pradip Deshmukh and Gayatri Satish Tikar</i>	
SYNCCODE: A SCALABLE REAL-TIME COLLABORATIVE CODING PLATFORM USING HYBRID OT-CRDT SYNCHRONIZATION AND WEBSOCKET ARCHITECTURE	111 - 126
<i>Adarsh Rana, Akshay Lodhi, Devansh Malik, Aviral Baliyan and Dr. Anurag Aeron</i>	
FEDERATED LEARNING FOR PRIVACY-PRESERVING DISEASE DETECTION IN DISTRIBUTED HEALTHCARE SYSTEMS	127 - 135
<i>Dev Kumar, Mohd. Zaid and Nikita Malik</i>	
SPENDWISE AI – SMART, PREDICTIVE, AND SUSTAINABLE EXPENSE MANAGEMENT SYSTEM	136 - 147
<i>Harsh Yadav, Khyati Sharma, Ishika Panwar, Simran Sehgal and Ms. Soni Panwar</i>	

A SECURE, SCALABLE AND INTELLIGENT ONLINE EXAMINATION SYSTEM USING AI-BASED PROCTORING AND ADVANCED ANALYTICS	148 - 162
<i>Nitin Dagar, Tushar Malik, Krishna Pandey and Gaurav Kumar</i>	
MINDSPHERE AI: AN INTELLIGENT MERN-BASED ADAPTIVE LEARNING AND KNOWLEDGE MANAGEMENT PLATFORM FOR DIGITAL FORENSICS AND CYBERSECURITY TRAINING	163 - 173
<i>Abhay, Aditya Yadav, Uday Gupta, Nishant Saini and Dr. Anurag Aeron</i>	
AI CHAT ASSISTANT USING MERN STACK: DESIGN, IMPLEMENTATION, AND PERFORMANCE EVALUATION OF A FULL-STACK NLP INTEGRATION	174 - 187
<i>Girjash Pratap, Devansh Pant and Priyanka Bhardwaj</i>	
DESIGN AND IMPLEMENTATION OF AN RFID-BASED AUTOMATED ATTENDANCE MANAGEMENT SYSTEM	188 - 204
<i>Aakrit Bansal, Ankit Goel, Anmol Tomar and Akash Kumar</i>	
UNIFIED MULTIMODAL AI SYSTEM FOR DECEPTIVE CONTENT DETECTION: INTEGRATING TEXT, IMAGE, AND URL ANALYSIS	205 – 211
<i>Shravani Kadam and Sudeshna Roy</i>	
AGROMIND: SMART FARMING USING MACHINE LEARNING MODELS	212 - 224
<i>Dr. Nidhi Poonia, Khushi Poojary, Paritosh Gaikwad and Aniket Singh</i>	
REAL-TIME CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING AND FASTAPI	225 – 233
<i>Professor Shravani Pawar, Pralhad Gaikwad and Atharv Vairagade</i>	

PAYMENT FRAUD DETECTION USING MACHINE LEARNING	234 - 243
<i>Prajjwal Pundir, Priyanshu Saini, Mayank Sharma, Lakshay Tyagi and Dr. Anirban Bhattacharya</i>	
KRUSHIMITRA BRIDGING LANGUAGE BARRIERS IN AGRICULTURE: A MULTILINGUAL AI-POWERED FARMING ASSISTANT	244 – 259
<i>Dr. Nidhi Poonia, Rajvardhan Ganpatrao Patil, Parshuram Das and Tanmay Padekar</i>	
A SMART TOKEN-BASED SYSTEM FOR AADHAAR SERVICES WITH REAL-TIME QUEUE TRACKING	260 - 279
<i>Mansi Patil, Shubham Yadav, Snehal Upadhyay and Rasika Patil</i>	
VANRAKSHAK: AI-BASED WILDLIFE MONITORING SYSTEM USING ML MODELS	280 – 288
<i>Professor. Shravani Pawar, Sudhir Morchale and Prathamesh Shinde</i>	
AI OPTIONS TRADER – ADVANCED MULTI-TIMEFRAME ENSEMBLE SIGNAL ENGINE	289 - 300
<i>Prof. Sudeshna Roy, Aniket Prakash Chougule and Suraj Jadhav</i>	
A COMPARATIVE STUDY OF MACHINE LEARNING MODELS FOR CHILDHOOD OBESITY RISK PREDICTION USING ANTHROPOMETRIC, LIFESTYLE, AND SOCIOECONOMIC DATA	301 – 313
<i>Dr Nidhi Poonia, Gayatri Mahajan, Aarti Pansare and Tanishq Praveen Chand</i>	
A MICROSERVICES-BASED SMART WASTE MANAGEMENT FRAMEWORK FOR REAL-TIME MONITORING AND ANALYTICS	314 – 327
<i>Mr. Omkar Pendkalkar and Professor Shravani Pawar</i>	

PRECISION AGRICULTURE: MULTI-CROP PLANT DISEASE DETECTION VIA HIERARCHICAL DEEP LEARNING AND QUANTIZATION-AWARE OPTIMIZATION	328 – 336
<i>Yashu, Vijay Kumar, Yash Tyagi Himanshu Rajveer and Miss Parul Kashyap</i>	
SMART GARBAGE MONITORING SYSTEM: A COMPREHENSIVE AI-DRIVEN IOT FRAMEWORK FOR INTELLIGENT WASTE MANAGEMENT	337 – 351
<i>Ritika Chaudhary, Sambhav Maheshwari, Shivam Singh, Khushi Sharma and Ms. Ritu Singh</i>	
DATA SECURITY AND PRIVACY IN CLOUD COMPUTING	352 – 361
<i>Ganesh Yashwant Sargar, Dr. Jyoti Kharade, Prashant Suresh Singh and Sayali Arun Bhamare</i>	
AI-BASED UTENSIL DEMAND FORECASTING SYSTEM FOR RENTAL SERVICES	362 – 373
<i>Ms.Shubhangi Mahadik, Mr.Sahil Sonawane and Mr.Manas H. Pemmi</i>	
COMPARATIVE ANALYSIS OF AI-DRIVEN TOOLS FOR PRONUNCIATION AND VOCABULARY ENHANCEMENT	374 – 382
<i>Professor Manish Dubey, Safal Sheray, Aniket Mokal, Amritsagar Mahapatra and Diptesh Chakraborty</i>	
A MINIMAL FEATURE APPROACH TO WEATHER PREDICTION USING ML	383 – 395
<i>Khushi Vinod Jaiswal, Soniya Gorakh Salunkhe and Professor Shubhangi Mahadik</i>	
A STUDY OF SOCIAL MEDIA ADDICTION IN STUDENTS USING BEHAVIORAL AND DEMOGRAPHIC DATA THROUGH A WEB-BASED SYSTEM	396 – 409
<i>Dr. Nidhi Poonia, Amruta Patil and Nidhi Sakpal</i>	

CAMPUS CONNECT: A MOBILE-BASED CENTRALIZED EVENT AGGREGATOR FOR COLLEGE COMMUNITIES	410 – 420
<i>Professor Shravani Pawar, Viraj Patil and Piyush Sontakke</i>	
SUGARCANE PROCUREMENT MANAGEMENT USING BLOCKCHAIN	421 - 429
<i>Professor Pratibha Deshmukh, Pankaj Desai, Siddaiah Bandrevu and Sakshi Rajendra Bhoge</i>	
SAFEGUARD AI: A REAL-TIME WARNING SYSTEM FOR DETECTING FRAUDULENT MEDIA CONTENT USING MACHINE LEARNING	430 – 439
<i>Manish Dubey, Kaif Khan, Sakshi Mishra and Harish Kumar</i>	
AI COURT ASSISTANCE APPLICATION (SMART JUSTICE): AN INTELLIGENT FRAMEWORK FOR JUDICIAL SUPPORT USING ARTIFICIAL INTELLIGENCE	440 – 461
<i>Rasika Patil, Yash Patil and Sayli Desai</i>	
OPERAT-O-FARM: A HYBRID AGGREGATOR FOR AGRICULTURAL MACHINERY WITH E-RUPI BASED SUBSIDY REDEMPTION AND WORKFORCE MANAGEMENT	462 – 469
<i>Dr. Shambhu Shankar Rai, Sumit Rane, Akash Prajapati and Samiksha Phadke</i>	
PRIVACY GUARD WEBSITE: A WEB-BASED SYSTEM FOR DETECTING AND PREVENTING DATA PRIVACY RISKS IN ONLINE APPLICATIONS	470 – 480
<i>Dr. Pratibha Deshmukh, Shivraj Mahatme and Anjali Rathod</i>	
ENHANCING ACADEMIC DECISION-MAKING THROUGH PCA, SENTIMENT-ANALYSIS AND TOPIC-BASED ANALYSIS OF RATING-BASED STUDENT FEEDBACK	481 – 491
<i>Vedant Pawar and Dr. Priya Chandran</i>	

AN INTELLIGENT MOBILE PLATFORM FOR DISCOVERING AND ACCESSING WOMEN'S WELFARE SCHEMES USING AI AND SMART FILTERING	492 - 501
<i>Prof. Dr Priya Chandran, Sanika Darge and Prachi Patil</i>	
NEUROPROMPT: AN INTELLIGENT AI-BASED DEBUGGING ASSISTANT FOR AUTOMATED ERROR ANALYSIS AND RESOLUTION	502 – 517
<i>Prof. Dr Priya Chandran, Mayur Musale and Vaishakh Banawalkar</i>	
UNIFIED PRIVACY-PRESERVING FRAMEWORK FOR WEB-BASED MESSAGING: MITIGATING VISUAL EAVESDROPPING AND UNAUTHORIZED LOCAL ACCESS	518 – 526
<i>Raj Singh, Mrs. Shravani Pawar and Atharv Tandel</i>	
SAFEWHEELS: AN INTEGRATED SMART DRIVER MONITORING SYSTEM FOR REAL-TIME DROWSINESS AND ALCOHOL DETECTION	527 – 537
<i>Prof. Rasika Patil Surbhi Dev and Avadhut Dhulugade</i>	
A PARALLEL SMART-DIVIDE MERGE SORT: AN ADAPTIVE AND SCALABLE FRAMEWORK FOR MULTI-CORE SYSTEMS	538 - 549
<i>Suhasini Vijaykumar, Siddhesh Ganesh, Vinit Sawant and Kaustubh Tambe</i>	
A NOVEL DEEP LEARNING APPROACH FOR REAL-TIME SIGN LANGUAGE GESTURE-TO-TEXT CONVERSION USING CNN-LSTM WITH NLP-BASED SENTENCE REFINEMENT	550 – 562
<i>Kirthi G Shetty, Raj Singh, Paarth S Tamgale, Shivam S Shinde and Rasika Thakare</i>	

A SMART LOCATION INTELLIGENCE PLATFORM FOR REAL-TIME MONITORING OF NEARBY PUBLIC AND COMMERCIAL SERVICES TO ENHANCE TRAVEL EFFICIENCY AND USER EXPERIENCE	563 - 569
<i>Manish Dubey, Sakshi Jaiswal and Satyam Jaiswal</i>	
USE OF ARTIFICIAL INTELLIGENCE IN CARDIAC ARREST	570 - 577
<i>Manish Dubey, Saloni Basare and Nikita More</i>	
IPFS CONTENT ADDRESSING WITH BLOCKCHAIN VERIFICATION	578 – 586
<i>Abhishek Yewale and Dr. Suhasini Vijaykumar</i>	
MALWARE DETECTION USING MACHINE LEARNING	587 – 597
<i>Dr. Suhasini Vijaykumar and Anjali Manoj Singh</i>	
AN INTELLIGENT IOT-BASED SMART HOME SECURITY SYSTEM USING REAL-TIME LOGGING AND LIGHTWEIGHT MACHINE LEARNING FOR ANOMALY DETECTION	598 – 609
<i>Rajat Kshirsagar and Vaishnavi Ingle</i>	
HEALTHY FOOD: A SMART THALI-BASED PERSONALIZED NUTRITION RECOMMENDATION SYSTEM	610 – 618
<i>Mansi Kumbhar, Dr. Suhasini Vijaykumar and Aaradhana Rajbhar</i>	
REDUCING CODE UNDERSTANDING TIME IN ENTERPRISE SYSTEMS USING AN AI-BASED CLI DOCUMENTATION TOOL	619 – 627
<i>Ninad Jambhale and Abhishek Mhamane</i>	
SPOTZY – SMART PARKING MANAGEMENT AND SLOT RESERVATION SYSTEM	628 - 642
<i>Dakshraj, Daksh Yadav, Dakshita Mishra, Shantanu Tyagi and Ms. Sapna Singh</i>	

AI-BASED BONE AGE PREDICTION THROUGH LEFT HAND X-RAYS 643 – 653

Dr. Jyoti Kharade, Ashish Ashok Singh, Dr. Shambhu Shankar Rai and Abhishek Gase

WEB-BASED MEDICAL SYMPTOM ANALYZER FOR DISEASE PREDICTION USING DATA ANALYTICS AND MACHINE LEARNING IN HEALTHCARE INFORMATICS 654 – 665

Prof. Sudeshna Roy, Ramavtar Varma, Harshad Bagal and Ganesh Kodi

REAL-TIME PHISHING DETECTION USING XGBOOST 666 – 674

Pranali Samarth and Syed Raquim Hussain Naqvi

FLOWGUARD:- AN AI POWERED PACKET CLASSIFICATION AND INTRUSION DETECTION USING INTELLIGENCE FRAMEWORK. 675 - 678

Mr. Shivam Anil Khaw and Mr.Omkar VishnuDahifale

MACHINE LEARNING-BASED PREDICTION OF DRUG SOLUBILITY IN MULTI-COMPONENT DRUG-SOLVENT SYSTEMS 679 - 693

Pranali Palve, Dr. Priya Chandran, Prathamesh Gharat and Dr. Suhasini Vijaykumar

ROLE OF AI IN ENHANCING TRAVEL SAFETY SECURITY AND CRISIS MANAGEMENT IN INDIA 694 – 703

Saroj Sharma and Prof K K Shukla

HUMAN FACE RECOGNITION SYSTEM USING DEEP LEARNING 704 - 719

Aditya Singh, Akash Ujjwal, Yatharth Kumar and Yash Poonia

COMPARATIVE EVALUATION OF MACHINE LEARNING AND ENSEMBLE MODELS FOR EARLY DETECTION OF POLYCYSTIC OVARY SYNDROME (PCOS)

Shreya Gupta¹, Shreya Bhandari², Smridhi Katyal³, Khyati Alhawat⁴, Sakshi⁵
and Jagriti Singh⁵

^{1,2,3,4,5}Department of Computer Science and Engineering Indira Gandhi Delhi
Technical University for Women (IGDTUW) Delhi, India

shreyajune19@gmail.com¹, shreyabhandari423@gmail.com²,
smridhi.katyal24@gmail.com³, khyatiahlawat@igdtuw.ac.in⁴,
sakshi1580101@gmail.com⁵, jagriti@igdtuw.ac.in⁶

ABSTRACT

Polycystic Ovary Syndrome is a complex disorder created due to hormonal imbalance when ovaries release high levels of androgens and is one of the most prevalent hormonal disorders which occurs in one in ten women of reproductive age. It is typically associated with the imbalance in menstrual patterns of women, unwanted facial and body hair, obesity, and insulin resistance and one of the reasons for infertility in women. Timely diagnosis helps women to make change in lifestyle and clinical interventions. For this study, we are using the Kaggle dataset which is from a hospital in Kerala, India. For identifying one of the most important features, advanced techniques such as Chi-square, Mutual information, and a hybrid LASSO Support Vector Machine Recursive Feature Elimination (SVMRFE) were implemented. For the models we used algorithms such as Gradient Boosting, AdaBoost, Random Forest, Logistic Regression and Support Vector Machines. To make the implementation more generalized, ensemble techniques - hard voting, soft voting and stacking classifier were introduced. This study highlights the machine learning framework to help diagnose the PCOS early and accurately.

Keywords— Polycystic Ovary Syndrome, Machine Learning, Ensemble Learning, SMOTE, Women's Health, Predictive Analytics Introduction

I. INTRODUCTION

Polycystic ovary syndrome is disruption in endocrine glands that imbalances the production of the sex hormones. In this condition, some people develop small fluid-filled near the ovarian outer surface. These are called cysts and contain undeveloped egg follicles which fail to regularly release eggs causing irregular menstrual cycles. It is not a necessary symptom of PCOS [1]. Data from Rashtriya Kishor Swathya Karyakram programme states that about 18% of women suffers from this disorder with around 70% cases remain untreated [2]. This is also linked to many metabolic diseases such as type 2 diabetes, obesity, insulin resistance, and cardiovascular diseases [3-4].

Diagnosis of PCOS accurately depends on the multiple diagnostic examinations conducted by qualified medical personnel. It becomes formidable in the areas where the health infrastructure is particularly deficient [5].

It also presents other challenges including overlapping symptoms and its heterogenous behavior. This raises the need for forecasting models that provide outcomes based on learning recognition and patterns to aid in the early diagnosis of the disorder [6-7]. Several scholars have carried out studies that demonstrate the potential of ML and Deep Learning for the predictions of PCOS. Rahman et al. suggested a web-based ML structure to aid in the PCOS detection using the structured clinical data [1]. Uddin et al. compared traditional and ensemble machine learning techniques and found that Random Forest and Gradient Boosting achieved better accuracy for early diagnosis [5].

On the statistical and classical ML side, Gupta et al. [11] used discriminant analysis for PCOS classification, with 95.9% test accuracy, while Joshi et al. [12] expanded this to a Deep LDA architecture using GPU acceleration for high dimensional data. Chen et al. [15] combined transcriptomic data with machine learning and found diagnostic biomarkers such as CNTN2, CASR, CACNB3, and MFAP2 through a hybrid LASSO, SVM, RFE pipeline. This work emphasizes the biological interpretability of machine learning in PCOS.

Other studies have investigated ensemble techniques, stacking, and explainable models for improved reliability in clinical decision-making [9], [13], [16], [20].

This paper proposes a transparent, feature-driven machine learning framework for PCOS prediction that includes clinical, hormonal, and lifestyle attributes. The most discriminative predictors, such as LH (mIU/mL), PRG (ng/mL), weight gain (Y/N), hair growth (Y/N), skin darkening (Y/N), fast-food (Y/N), and follicle count (L/R), were identified using three feature-selection techniques:

Chi- Square, Mutual Information, and hybrid LASSO + SVM- Recursive Feature Elimination [5], [11].

Multiple classifiers were trained and evaluated (Gradient Boosting, Random Forest, AdaBoost, Logistic Regression, SVM, and KNN), followed by ensemble and optimization comparisons.

This study demonstrates that a computationally efficient, interpretable, and dependable framework for PCOS detection is provided by robust feature selection in conjunction with optimized boosting. [10], [14], [20], [17].

II. LITERATURE SURVEY

The screening of Polycystic Ovary Syndrome with the use of machine learning techniques has made amazing progress in some previous years, particularly in the application of it on structured clinical datasets. The optimization algorithms such as stacking and ensemble have given often results of 99% accuracy, when applying on tabular data [2, 7, 5]. Also, some studies have also explained the importance of

feature selection techniques which lead to increase in the diagnostic performance, one of the methods commonly used is Mutual Information [1].

However, there are some challenges faced such as model interpretability and clinical adoption. There are many models which are highly accurate, but they provide less transparency about the reasoning and explanation behind the predictions.

There are other diagnostic approaches such as using imaging data -ovarian ultrasound scans they have not achieved reliability as compared to existing approaches. Some accuracies have range between 70% and 92% [17, 16], which explains the difficulty of extracting the features from ultrasound images. There is recent research which highlighted the growth of interest in the development of machine learning frameworks for PCOS diagnosis which are both transparent and explainable. Research Studies that used advanced models such as XGBoost for the prediction gave highly efficient results with more clinical understanding [15, 11, 16].

III. DATASET

The dataset which is used for analyzing Polycystic Ovary Syndrome (PCOS) in this study is from a public clinical data collection shared by Prasoon Kottarathil on the Kaggle platform. It consists of a medical record of 541 female patients which were gathered from ten separate hospitals in state Kerala, India. The dataset provides a field for analysis, which has 45 variables that capture the major clinical and physiological factors associated with PCOS. The body measurement indicators such as Age and BMI, metabolic health indicators such as glucose and insulin levels, and sex indicators such as FSH, LH and Testosterone. Also, the patient clinical reporting includes hirsutism, acne, menstrual cycle irregularities etc. PCOS diagnosis is represented in the binary format -1 for PCOS detection and 0 for non- PCOS.

This dataset provides structured clinical, hormonal characteristics combined with the lifestyle features making it more relevant for the prediction

IV. METHODOLOGY

This study follows systematic analysis -collecting the dataset and extracting relevant features from the data to utilize them into the model. These steps ensure the reliability of the model and helps to improve the prediction performance.

A. Data Exploration and Preprocessing

Data exploration and preprocessing involve examining the dataset and preparing for the model training.

1) Data Cleaning

Data cleaning has a significant part in ensuring that the model performs efficiently. The dataset used in this study includes 541 records and 45 attributes to cover all the clinical, hormonal, and lifestyle factors of the patients. During preprocessing, we removed the columns that were no longer needed, like “Unnamed: 44.” For missing number values, we filled them with the median, and for missing text values, we used

the mode. Yes/No-type answers (like Y/N or R/I) are changed into 1 and 0 so the computer can understand them

Outliers were identified and handled using the Interquartile Range (IQR) technique to prevent extreme values from influencing the model's performance.

2) Tools and Techniques

This experiment was conducted using Python 3.9.13 on a Windows 10 system, with the support of 11 th Gen, an Intel Core i5 processor and 8 GB RAM. Data preprocessing and numerical operations were supported by Pandas and NumPy, whereas visualization and exploratory analysis were mainly done by Matplotlib and Seaborn.

3) Balancing the Dataset

The original data had an uneven distribution problem where there were 364 non-PCOS cases and 177 PCOS cases. To handle this situation, Synthetic Minority Oversampling Technique (SMOTE) was applied.

4) Feature Selection

Feature selection is a vital process to improve model accuracy, interpretability, and computational efficiency. The research employed three hybrid feature selection methods: Chi-Square with XGBoost, Mutual Information with Random Forest, and SVM-RFE after LASSO regularization.

- Chi-Square + XGBoost: The Chi-Square test measures the strength of the association between each feature and the target class, whereas XGBoost shows feature importance based on its gradient boosting decision trees. The union of these two methods allows for the identification of features that are significant from the statistical point of view.

Table 1. Top 15 Features (Chi-Square + Xgboost)

Rank	Feature Name	ChiSquare Score
1	Skin darkening Y/N	78.65
2	Hair growth Y/N	70.24
3	Weight gain Y/N	62.11
4	Fast food Y/N	50.32
5	Follicle No R	47.10
6	Follicle No L	43.27
7	Cycle R/I	39.84
8	Pimples Y/N	20.15
9	Blood Group 16	15.23
10	Blood Group 15	13.54
11	Pregnant Y/N	9.80
12	AMH ng/mL	8.90
13	No of abortions	7.45
14	Vit D3 ng/mL	6.73
15	Blood_Group_17	6.51

- **Mutual Information + Random Forest:** Mutual Information measures the dependency between variables by calculate the amount of information they share, while Random Forest ranks them through its ensemble-based learning process. Together, this approach provides a balanced view by combining statistical relevance with model driven evaluation.

Table II. Top 15 Features (Mutual Information+ Random Forest)

Rank	Feature Name	Mutual Info Score
1	Follicle No R	0.28
2	Follicle No L	0.25
3	Avg F size R mm	0.18
4	Avg F size L mm	0.17
5	Hb g/dl	0.16
6	Fast food Y/N	0.14
7	Marriage Status Yrs	0.13
8	AMH ng/mL	0.12
9	Height Cm	0.11
10	Cycle length days	0.10
11	PRG ng/mL	0.09
12	Waist:Hip Ratio	0.08
13	Endometrium mm	0.07
14	Skin darkening Y/N	0.06
15	Hair growth Y/N	0.05

- **SVM-RFE (Applied After LASSO) :** LASSO was used to remove redundant before RFE was applied. The Support Vector Machine–Recursive Feature Elimination method iteratively drops features that have the least impact, which is decided by the weight coefficients of the SVM model. This two-step process produced a cleaner and more optimized feature set for model training.

Table III. Feature Ranking By Svm-Rfe (After Lasso)

Rank	Selected Feature	Description
1	Weight_gain_Y/N	Indicates weight change associated with PCOS
2	Hair_growth_Y/N	Represents hirsutism symptom
3	Skin_darkening_Y/N	Related to insulin resistance
4	Fast_food_Y/N	Dietary factor linked to PCOS risk
5	PRG_ng/mL	Progesterone hormone level
6	LH_mIU/mL	Luteinizing hormone level
7	Follicle_No_L	Right ovary follicle count
8	Follicle_No_R	Left ovary follicle count
9	Cycle_R/I	Menstrual cycle regularity
10	Blood_Group_13	Patient blood group

B. Machine Learning Techniques

Multiple machine learning algorithms were developed and compared. Each model was trained on the cleaned and balanced dataset, and their performance was assessed using a range of evaluation metrics.

1) Logistic Regression

Logistic Regression served as the baseline model against which other models were compared and generally applied to the binary classification problems. The model calculates the probability of a given instance belonging to a certain class by passing the linear combination of the input features through the sigmoid (logit) function.

$$y = \frac{1}{1 + e^{-(B\{0\} + B\{1\}x\{1\} + \dots + B\{n\}x\{n\})}} \quad (1)$$

2) Decision Tree

The Decision Tree classifier structures the data in a hierarchy resembling a tree and divides it at various points depending on feature values. In this way, the model becomes easily interpretable and can be used to identify the most influential features for the predictions. Despite the fact that Decision Trees may overfit, they still offer a clear insight into the decision process and the routes that result in each classification.

3) Random Forest

The Random Forest is constructing several decision trees using some random subsets of the data and then aggregates all the predictions. Such an ensemble strategy elevates the precision of the model and is a good way to hedge against overfitting. The random choices in both sampling and feature selection make the model stronger. Besides that, Random Forest can give valuable insights regarding the most important features, which facilitates interpreting the results.

4) Gradient Boosting

Gradient Boosting sequentially trains a series of weak learners, where each new model tries to fix the errors of the previous one. It was effective overall in this research, obtaining an accuracy of 93.84% with features selected by Mutual Information and 94.52% with features selected by the Chi-Square method.

5) AdaBoost

AdaBoost works with weak learners by raising the weights of those samples that are misclassified at every iteration; thus, the following models are "forced" to pay more attention to the difficult cases. This method results in better general performance and to a higher power of the model. In our trials, AdaBoost recorded an accuracy of 91.10% and its performance was very consistent across different samples.

6) Support Vector Machine (SVM)

SVM identifies building decision boundary that separates the two classes with the maximum possible margin. It used the RBF kernel to identify non-linear patterns in the data. Nonetheless, its performance was a bit lower (82.19%) mainly due to the fact that SVM models are highly sensitive to parameter tuning and the occurrence of outliers.

7) K-Nearest Neighbors (KNN)

KNN labels classify the training data that most frequently occurs among its closest neighbours in the feature space. The model achieved an accuracy of 86.30%.

C. Train-Test Split

The data was divided into two parts, training (80%) and testing (20%) sets, through stratified sampling so that the class distribution was maintained.

D. Ensemble Learning Techniques

Three ensemble learning techniques—Hard Voting, Soft Voting, and Stacking—were applied to enhance the generalization of the predictive framework. The power of these single classifiers is increased by the methods which combine the results of several base models and they also make the errors of the individual classifiers less.

1) Hard Voting

Under Hard Voting, every classifier gives a vote for a class label, and the class that gets the most votes is the final prediction. Here, the three base models are represented by Logistic Regression, K-Nearest Neighbors, and Decision Tree.

2) Soft Voting

The soft-voting operate works on the average of the class- probability predictions of multiple classifiers and assigns to the final label based on the highest average probability. In this setup, Random Forest, Gradient Boosting, and Logistic Regression were mixed.

3) Stacking Classifier

Stacking is a method that integrates the results from several base classifiers through a meta-learner that is trained on their outputs. Here, Logistic Regression is the meta-learner and Decision Tree, Support Vector Machine, and Logistic Regression are the base models.

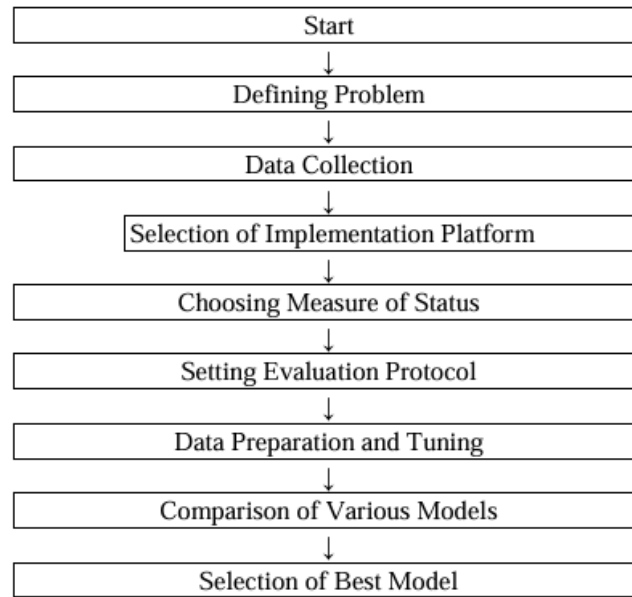
Overall, the three ensemble approaches such as Soft Voting, Hard Voting and Stacking are improved both the predictive accuracy and strength of the system. Among them, the Stacking classifier and Soft Voting has results, achieving accuracies of 93.84% and 93.83%, respectively, and outperforming the individual models.

V. COMPARED APPROACHES

To identify the most effective model for PCOS detection, multiple machine learning algorithms were trained with the help of feature selection using Mutual Information and Chi Square selection methods. Overall, the ensemble models provided better accuracy and stability than the individual classifiers. Gradient Boosting emerged as the more effective model showing optimal performance - accuracy of 93.84%. Random Forest gives an accuracy of 92.47% followed by AdaBoost accuracy - 91.10%. Logistic Regression demonstrated 88.36 accuracy that offers simplicity, but not flexible enough to model complicated patterns. Decision Tree (84.25%) and KNN (86.30%) gives the moderate results as Decision Tree is more tend to overfit. The SVM model got 82.19% which is a sensitivity of the model under concerns of the kernel settings and outliers.

Soft Voting and Stacking are the ensemble methods demonstrating accuracy is 93.8% surpassing the Hard Voting method (90.41%) due to their strong generalization and stable performance. The Gradient Boosting gave the best accuracy of 94.52 with the Chi-Square feature selection process.

Fig.1. Flowchart of the Proposed Methodology



VI. EXPERIMENTAL STUDIES

A. Experimental Setup

The experimental work was implemented in the computer having Intel Core i7 CPU, 16 GB of main memory, and running Windows 11. The language and the libraries utilized in this work were Python 3.10 as programming language and Scikit-learn, Pandas, NumPy , and Matplotlib.

B. Evaluation Metrics

The performance of the machine learning models was assessed using standard classification metrics:

Table IV. Evaluation Metrics

Metrics	Formula
Accuracy	$(TP + TN) / (TP + TN + FP + FN)$
Precision	$TP / (TP + FP)$
Recall	$TP / (TP + FN)$
F1-Score	$2 \times (Precision \times Recall) / (Precision + Recall)$

C. Results and Discussion

Various machine learning algorithms such as Logistic Regression, Random Forest, Decision Tree, Support Vector Machine (SVM), and XGBoost were trained and compared.

Table V. Accuracy, Precision, Recall, F1-Score Of Various Models

Model	Accuracy	Precision	Recall	F1-Score
Logistic Regression	84.3%	82.5%	83.6%	83.0%
Decision Tree	86.1%	85.2%	84.7%	84.9%
Random Forest	92.5%	91.8%	92.1%	91.9%
SVM	88.9%	87.6%	87.9%	87.7%

With an accuracy of 92.5%, the Random Forest has best overall performance. Random Forest's ensemble features generalize well and decrease the overfitting. The confusion matrix study, which showed a low number of false negatives, shows that the model is reliable for medical diagnostic applications where missing a positive instance could have serious consequences.

VII. CONCLUSION AND FUTUTRE SCOPE

A. Conclusion

This study demonstrates the application of Machine Learning algorithms for predicting Polycystic Ovary Syndrome (PCOS) using clinical and hormonal data. The results validates that ML-based decision support systems can assist healthcare professionals in early and accurate PCOS detection, which will lead to timely patient treatment and better outcomes.

B. Future Scope

Future research can be directed more towards the areas:

- **Larger and Multi-source Datasets:** Integrating data from large numbers of hospitals or regions and areas to enhance model generalization.
- **Explainable AI (XAI):** By analysing the model predictions using techniques like SHAP or LIME, this will improve the clinician's trust.
- **Real-Time PCOS Prediction System:** Developing a mobile or web application that provides patients with an instant risk assessment.
- **Integration with IoT Devices:** Using information from different wearable health trackers to continuously monitor the hormonal and physical indicators.

REFERENCES

- [1] Rahman, M.M. et al., "Empowering early detection: A web-based ML approach for PCOS prediction," *Informatics in Medicine Unlocked*, 47, 2024J.
- [2] Umaa Mahesswari, G. & Uma Maheswari, P., "SmartScanPCOS: Feature-driven ML and XAI-based prediction of PCOS," *Heliyon*, 2024.K. Elissa, "Title of paper if known," unpublished.
- [3] Khanna, V.V. et al., "Explainable ML framework for PCOS detection," *Manipal Institute of Technology, India*.Y.
- [4] Zad, Z. et al., "Predicting PCOS with ML using EHR data," *Frontiers in Digital Health, USA*.
- [5] Uddin, K.M.M. et al., "Early PCOS detection via traditional and ensemble ML models," *Engineering Reports, Wiley*, 2025.
- [6] Nasim, S. et al., "PCOS prediction using ML in bioinformatics," *IEEE Access*, 10, 2022
- [7] Moral, P. et al., "CystNet: AI-driven PCOS detection from ultrasound images," 2024.
- [8] Mridul, A.H. et al., "PCOS prediction using ML and deep learning," *IJCISIMA*, 16, 2024.
- [9] Lim, J. et al., "ML classification of PCOS via pulse wave analysis," *BMC Complement. Med. Ther.*, 23, 2023.
- [10] Panjwani, B. et al., "Optimized ML for early PCOS detection," *Sensors*, 23, 2023.
- [11] Agirsoy, M. & Oehlschlaeger, M.A., "Non-invasive PCOS diagnosis using ML," *Scientific Reports*, 14, 2024.

-
-
- [12] Gupta, A.M. et al., “Discriminant analysis for PCOS prognostication,” Univ. of Mumbai, 2022.
- [13] Joshi, R. et al., “Deep LDA variation for PCOS classification,” Univ. of Mumbai, 2022.
- [14] Hosain, A.K.M.S. et al., “PCONet: CNN-based PCOS detection from ultrasound,” BRAC Univ., 2023.
- [15] Wang, J. et al., “AI in PCOS management: past, present, future,” *La Radiologia Medica*, 130, 2025.
- [16] Sowmiya, S. et al., “F-Net: Deep learning tool for PCOS diagnosis,” *PLOS ONE*, 20(2), 2025.
- [17] Chen, W. et al., “ML models for PCOS biomarkers and immune analysis,” *J. Ovarian Research*, 18, 2025.
- [18] Divekar, A. & Sonawane, A., “AI-based automatic PCOS classification,” VIIT Pune, 2025.
- [19] Kermanshahchi, J. et al., “ML-based PCOS detection from pelvic ultrasound,” *California Univ. of Science and Medicine*, 2025.
- [20] Suha, S.A. & Islam, M.N., “Extended ML for PCOS detection using ultrasound,” *Scientific Reports*, 15, 2025.
- [21] Shanmugavadivel, K. et al., “AI-based prognosis and classification of PCOS,” *BMC Med. Inform. Decis. Making*, 24, 2024.
- [22] Denny, A. et al., “i-HOPE: ML-based PCOS detection and prediction,” *Sahrdaya College of Engg. & Tech.*, 2025.

ML POWERED STUDENT PERFORMANCE ANALYSIS SYSTEM

Dr. Shambhu Shankar Rai¹, Priyanka Dharade² and Darshan Hodage³

¹Assistant Professor, Bharati Vidyapeeth's Institute of Management and Information Technology, Belapur

^{2,3}MCA, Bharati Vidyapeeth's Institute of Management and Information Technology, Belapur

[¹shambhumca1@gmail.com](mailto:shambhumca1@gmail.com), [²priyankadharade2003@gmail.com](mailto:priyankadharade2003@gmail.com) and [³hodagedarshan@gmail.com](mailto:hodagedarshan@gmail.com)

ABSTRACT

To Predict about how students will perform and finding who will struggle in school is very important for schools. Teacher's uses grade and attendance for verify students. Which do not every time show the full picture of their learning.

This article presents a system which is using a machine learning to analyze student performance by looking their behavior, grades and lifestyle. The system groups students into three Level of risk: low, medium and high. It works on various factors like attendance, assignment, exam scores, and hours of study, sleep hours, phone use, confidence and stress level. A Random Forest classifier is used to make decision because it's reliable and may able to handle many factors.

The system is analyzing the teacher comments also for student's emotions identify. A web application is which is using Python, HTML5, CSS, JavaScript and Chart.js. Students and teachers can watch on dashboard for performance trends, lifestyle analysis and customized study plans. Experiment results indicates that this system can correctly identify students who might need help .It can help teachers and management to take timely decisions for improve performance and minimize the risk of students drop out.

Index Terms—Student's Dropout Prediction, Machine Learning, Educational Data Mining, Academic Risk Analysis, Learning Analytics

I. INTRODUCTION

Student performance evaluation is the part of managing academics in school and college. Traditionally it was measuring by looking at Student's exam results, attendance records and assignments they had submitted. These things do give us some information but they do not always show the complete picture of how a student is learning. There are other important things like habits how long a student sleeps, student's stress level, their confidence and how much they use mobile phone which may affect their performance in school. If we ignore these things we may not really understand how a student is doing. With many students and academic systems getting more complex it has become hard for teachers to keep track of each student's

progress. Often a student struggles when their performance has already gone down a lot. Finding out late that a student is struggling makes it harder to help them. It can lead to bad grades, lack of motivation or even failing school. So we require a systems that can look at student data all the time and warn us if a student needs help.

New developments in machine learning and looking at data have made it possible to analyze a lot of student data and find patterns that mean something. Machine learning models can combine records with information about a student's behavior and lifestyle to predict how well they will do in school more accurately. These systems help schools find students who are struggling on and give them personalized help to improve their learning.

In this project we are proposing a system called ML Powered Student Performance Analysis System to deal with these issues. The system collects information about a student's academics and lifestyle such as attendance, internal marks, assignment scores, study hours, sleep duration, mobile usage, stress level and confidence level. We use a Random Forest classification model to predict if a student is at risk and we also analyze the tone of feedback from faculty members. The system is a web-based application with dashboards for students and faculty members. By putting prediction, visualization and feedback the system we propose aims to support helping students early improve how we monitor academics and make student performance better overall. Student performance evaluation and student performance are very important. The proposed ML Powered Student Performance Analysis System is designed to improve student performance.

II. BACKGROUND

Monitoring student performance is a responsibility for schools. Teachers usually look at how students do on tests if they come to class and if they turn in their work. This gives an idea of how they are doing but it does not show the whole picture of how they learn. How well a student does in school is not about what they do in class it is also about things like how they study how much they sleep how stressed they are and if they use digital devices too much. When we do not think about these things it is hard to know how a student is doing. Recently a lot of students have started going to college so it is harder for teachers to keep track of each student. Teachers have classes and a lot of work to do so they do not have a lot of time to help each student one on one. This means that sometimes we do not find out that a student is struggling until they are already doing poorly. If we find out late it is harder to help them and they might keep doing poorly lose interest in school or even quit.

At the time we now have a lot of digital records and online systems that give us a lot of information about students. We have records of who comes to class, test scores, assignments and feedback from teachers. This information is very useful for looking at how students are doing in a more organized way. However we need ways to look at all this data and find connections between different things that affect how students learn. Luckily machine learning and educational data mining have made it possible to

make academic monitoring systems better. Machine learning algorithms can look at a lot of student data find patterns that're not easy to see and predict how students will do in the future. By looking at behavioral and lifestyle-related information these systems can help schools find students who might do poorly before it happens. If we find out early teachers and administrators can give students the help they need.

This is why it would be very useful to have a system that uses machine learning to analyze student performance. Such a system could bring together information from sources use models to make predictions and show the results in a way that is easy to understand for both students and teachers. By giving us predictions of who might be at risk trends in performance and personalized advice the system can help us make decisions about academics and improve student learning outcomes and retention rates. The development of an ML Powered Student Performance Analysis System is very relevant. Student performance is what this system is, about. Student performance is the focus. By using this system we can look at student performance in a way and help students do their best. Student performance will improve if we use this system.

III. OBJECTIVE

The goal of this study is to create a system which uses machine learning to look at how students are doing and figure out if they are at risk of not doing well in school. This system will look at things like students grades on tests and assignments how many hours they study, how much they sleep how much time they spend on their phones how stressed they are and how confident they feel. Next goal is to make a model that can put students into groups based on how risk they are of not doing well in school. This way teachers can find out early which students are struggling. Understand more about how students doing in school and how they are feeling. The study wants to make a website that's easy to use, where students and teachers can see how students are doing. This website will show how students are doing over time what they are doing outside of class and if they are at risk of not doing. It will also give students plans for how to study and reports on how they're doing that they can download. The system will give students advice on how to study and make plans based on how they're doing and if they are at risk of not doing well. The system will also help teachers make decisions, about how to help students by giving them detailed reports and warnings when students are not doing well. The main goal of this study is to help students do better in school stop them from failing and make a system for schools to keep track of how students are doing. This system will help teachers catch problems early and make sure students get the help they need to succeed. The student performance and academic risk levels will be looked at closely to make sure the system is working.

IV. LITERATURE REVIEW

A. AI-Driven Predictive Model for Early Detection and Prevention of Student Dropouts [1]

V.Jean Shilpa, S. Sridevi and S. K. Ramamoorthy came up with an AI-driven model for the early detection and prevention of student dropouts. They used things like scores and demographic information to train machine learning classifiers. This model was really good at predicting student dropouts with an accuracy of around 92 to 94 percent. The good thing about this work is that it can identify students who're at risk of dropping out early on. However it did not look at lifestyle factors like stress or sleep. It also did not have a dashboard that students and teachers could use to keep track of performance.

B. AI-Based Identification and Support of At-Risk Students [2]

Ismail Elbouknify and others presented an AI-based system to identify and support at-risk students in Morocco. They used machine learning algorithms like Random Forest and Decision Trees to look at student records and engagement data. Their model was able to identify students who were likely to have difficulties and gave reliable results.. This system was mainly designed for a specific region and did not have a dashboard for students and faculty members to use.

C. Dual-Modal Abrupt Behavioral Changes Approach [3]

Jiabei Cheng and others had proposed a modal of deep learning approach that looked at academic performance and behavioral changes over time to predict student dropout risk. This model tracked changes in student engagement and performance and was able to predict dropouts with an accuracy of nearly 94 percent.. It needed continuous online learning data, which limits its use in offline educational environments. It also did not have a web-based interface for teachers and students.

D. AI-Powered Early Detection and Prevention System for Student Dropout Risk [4]

N. B. Mahesh Kumar and others had developed an AI-powered detection system that used a Flask-based web framework. Their model looked at things like attendance and grades and was able to predict dropouts with an accuracy above 90 percent. This work is similar to the proposed system because it combines machine learning with a web-based implementation. However it mainly focused on predicting risk. Did not have rich visualization features or separate dashboards for students and faculty members.

E. Predictive Models for Student Dropout in Teacher Education [5]

Marcel Jud, Barbara Weissenbacher and Aljoscha C. Neubauer conducted a study on predicting dropout among students enrolled in teacher education programs. They used machine learning models. Achieved accuracy levels of around 90 percent. Their study showed that machine learning models can work well in educational domains. However it was limited to teacher education programs. Did not look at lifestyle or emotional factors. It also did not have a dashboard-based monitoring system.

F. All-Year Dropout Prediction Modeling for University Students [6]

Zihan Song, Sang-Ha Sung, Do-Myung Park and Byung-Kwon Park proposed an all-year dropout prediction system for university students. They used algorithms like Logistic Regression and Support Vector Machines to analyze student data and achieved prediction accuracy of 91 percent. Although the model supported dropout prediction it mainly looked at academic and enrollment-related features. It did not look at behavioral or lifestyle-related attributes and did not have an interactive real-time dashboard.

G. Research Gap and Motivation

Even though existing systems are good at predicting student dropout risk there are some gaps. Most studies mainly look at data like marks and attendance and do not consider lifestyle and emotional factors like sleep, stress and mobile usage. Many systems are also developed for research and do not have real-time, web-based dashboards for students and teachers to use. There is also interaction between faculty and students as most systems are designed for administrators. Emotional and sentiment analysis features are rarely. Personalized guidance or study planning tools are often missing. Many existing approaches do not store long-term performance data. Provide effective visualizations. These limitations show the need, for an integrated, interactive and holistic student performance analysis system, which's what the proposed ML Powered Student Performance Analysis System aims to do.

V. PROBLEM STATEMENT

Schools usually look at how students do by checking their test scores, attendance and homework. This does not tell us everything about how a student learns because things like how they study, when they sleep how stressed they are how much they use their phone and how they feel are not considered. Because there are many students and teachers do not have a lot of time it is hard to find out which students are struggling early on. A lot of students are only found to be at risk when their grades have already gone down which means it is harder to help them and improve their grades. Most systems that try to predict how well students will do only look at their records and do not let students and teachers interact with them very much. They also do not make it easy for students and teachers to see the information and get advice.

There is no way to bring together academic, behavioral and lifestyle information and to get real-time updates and analysis. So we need a system that can look at student performance on the web and predict if a student is, at risk of doing poorly early on. This system should also help teachers and students make decisions based on the data and provide personalized guidance to improve how well students

VI. METHODOLOGY

Student Performance Analysis System which is using Machine Learning doesn't just look at grades. It studies at a lot of things e.g how students go to class how well they do on tests how much they study, how many hours they sleep how much time they

spend on mobile phones how stressed they are and what their teachers think about them.

This study tries to find out which student might be struggling in school by looking at all these things. It then shows the results in a way that's easy to understand on a website.

First the system collects all the information about the students. This includes things like attendance test scores and homework grades. It also looks at things like how much students study, how much they sleep and how time they spend on phones. All these things are important because they can affect how well a student does in the school.

Next the system makes sure all the information is correct and consistent. This means fixing any mistakes getting rid of information and making sure everything is in the right format. The system also splits the information into two groups: one for training and one for testing. This helps the system learn how to make predictions.

Then the system chooses the important information to use for making predictions. This helps the system make predictions and not get confused by too much information. The system uses both information, like grades and lifestyle information like sleep and study habits to get a complete picture of each student.

After that the system uses an algorithm called Random Forest to make predictions. This algorithm is good at handling a lot of types of information and is not easily fooled by random patterns. The system trains the algorithm using the collected information. Adjusts it to make the best predictions. The algorithm then puts students into three groups: risk, medium risk and high risk.

The system also looks at what teachers and students say about their experiences. It uses a technique to figure out if the comments are positive, negative or neutral. This helps the system understand how students are feeling and what they need to succeed.

The system is built using Python and other tools. It has a website that students and teachers can use. The website shows students their risk levels how they are doing over time and provides tools to help them plan their studies. Teachers can see how their students are doing and provide feedback

All the information is stored in a database, which helps the system keep track of everything over time. The system also uses tools to make graphs and charts that show the results in a way that is easy to understand.

Finally the system checks how well it is working by using measurements like accuracy and precision. This helps make sure the system is making predictions and is useful for helping students who are struggling. The whole system is designed to help schools identify students who need help and provide them with the support they need to succeed.

The Student Performance Analysis System is a tool that uses Machine Learning to help students. It looks at a lot of things to figure out which students might be struggling. The system is designed to be easy to use and provides a lot of information to help students and teachers. The Machine Learning part of the system is what makes it so good at making predictions.

The system is made up of different parts, including the Machine Learning algorithm, the database and the website. All these parts work together to provide a picture of each student and help them succeed. The Student Performance Analysis System is an example of how Machine Learning can be used to make a positive impact on people's lives.

The Machine Learning part of the system is very important. It is what allows the system to make predictions about which students might be struggling. The system uses a lot of types of information to make these predictions, including academic information and lifestyle information. This helps the system get a picture of each student and provide the best possible support.

The Student Performance Analysis System is a useful tool for schools. It helps them identify students who need help and provide them with the support they need to succeed. The system is easy to use and provides a lot of information to help students and teachers. The Machine Learning part of the system is what makes it so good at making predictions and providing insights.

Overall the Student Performance Analysis System is a tool that uses Machine Learning to help students. It is designed to be easy to use and provides a lot of information to help students and teachers. The system is made up of different parts, including the Machine Learning algorithm, the database and the website. All these parts work together to provide a picture of each student and help them succeed. The Student Performance Analysis System is an example of how Machine Learning can be used to make a positive impact, on peoples lives.

VII. SYSTEM ARCHITECTURE

The Student Performance Analysis System which uses Machine Learning is made up of various layers. It puts together data processing, machine learning and visualization on the web. First we collect data about students like how they do in school how they behave and how they live. We store this data in a format called CSV.

Then data cleanup which make sure it is the right size before we use it to teach a Random Forest model. This model helps us guess how students will do. We save the model and a web application made with Flask uses it when it starts up.

When students put their information into the student dashboard the Flask application uses the model we taught to guess if they are at risk. Shows them the results. It also shows them charts, plans for studying and ways to get better. The teachers have their dashboard where they can see how their class is doing look at risk charts and check tables to see how students are progressing.

We can also make reports, in PDF and CSV formats so we can keep records and look at them when we are not online. This way of doing things helps us guess how students will do show them information in a way that's easy to understand and keep an eye on how they are doing in school.

The way the system works is simple: we collect data clean it up teach the model and then use it to make guesses on the web like you can see in Figure 8. The Student Performance Analysis System and Machine Learning work together to make this happen.

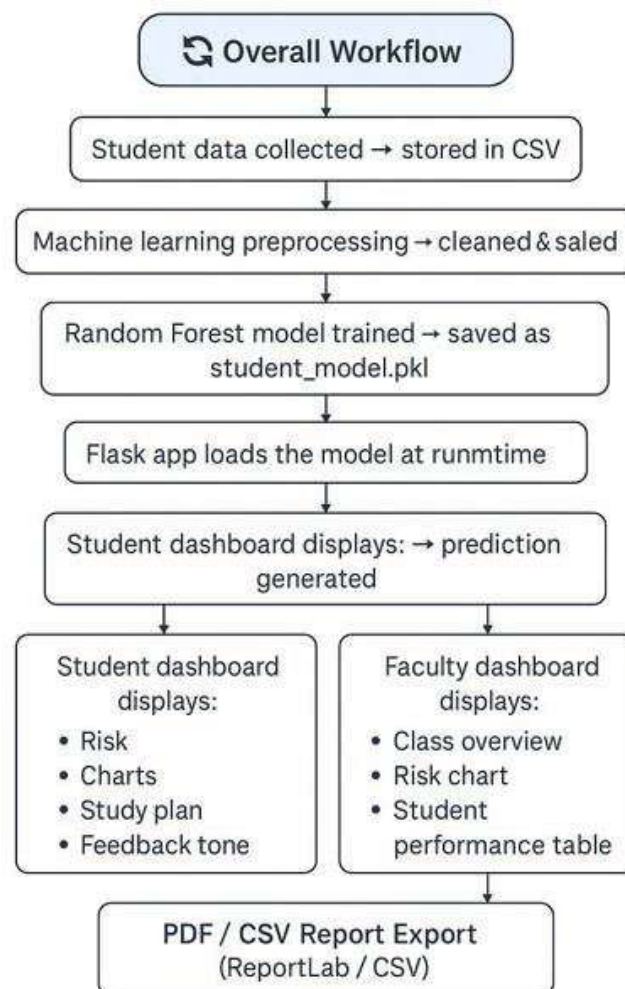


Fig.1. Overall Workflow of the Proposed Student Performance Analysis System

VIII. RESULTS ANALYSIS

A. Model Evaluation Setup

- The system we made was tested with a set of data that included information about students academic performance, behavior and lifestyle.
- We used a Random Forest classification model to figure out which students were at medium or high risk of doing poorly in school.

B. Performance Metrics

- We looked at how the model did by using standard measures like accuracy, precision, recall and F1-score..
- These measures helped us see if the model was making predictions and if it could identify students who were struggling.

C. Prediction Accuracy

- The results showed that the Random Forest classifier was really good at making predictions.
- This means that our system is good at finding students who are having trouble in school on.

D. Precision and Recall Analysis

- The model did not make false predictions, which means it was precise.
- It also correctly identified most of the students who were at risk which means it had recall.

E. F1-Score Performance

- The F1-score showed that the model was balanced between precision and recall.
- This balance means that the model is trustworthy for figuring out which students are at risk and for helping them on.

F. Real-Time System Testing

- We tested the system in time using the student dashboard and it worked well.
- The system showed charts of how the students were doing analyzed their lifestyle and even looked at the tone of their feedback.

G. Faculty Dashboard Analysis

- The faculty dashboard gave teachers an overview of their class including charts of which students were at risk and tables of student performance.
- This helped teachers keep track of how their students were doing and find students who needed help.

H. Visualization Results

- We used charts like bar charts and line graphs to help students and teachers understand how they were doing and which students were at risk.
- These charts made it easier for everyone to understand the results.

I. Report Generation

- The system made reports in PDF and CSV formats, which was helpful for looking at the data offline and keeping records.
- This feature also made it easy to share information about student performance with others.

J. Overall System Performance

- The results show that our system is good, at making predictions showing the data in a way and is easy to use.
- The system has a lot of potential to help teachers and students by providing warnings, personalized guidance and better ways to keep track of academic performance.



Fig.2.Student Dashboard– Prediction Risk Level, Semester Glance, and Why Risk



Fig.3. Student Dashboard– Academic Overview, Lifestyle Analysis, Progress Over Time

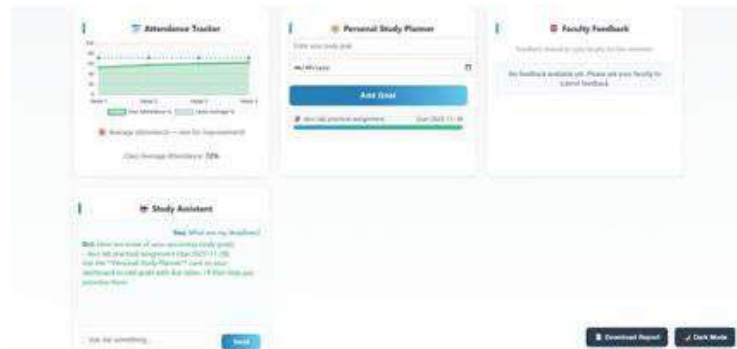


Fig.4. Student Dashboard– Attendance Tracker, Study Planner, Faculty Feedback, Study Assistant



Fig.5. Student Dashboard– Dark Mode



Fig.6. Faculty Dashboard– Update or Update Student Data



Fig.7. Faculty Dashboard– Class Overview

ML Student Performance System

Welcome, priyankadharade330@gmail.com

Download CSV | Dark Mode | Logout

Upload or Update Student Data

Student ID

Attendance %

Internal Marks %

Assignment Score %

Predict Risk

Fig.8. Faculty Dashboard– Dark Mode

IX. CONCLUSION

This paper presents the Student Performance Analysis System that uses Machine Learning to predict risk levels. It helps identify students who may face learning difficulties .

The system looks at records and factors like behavior and lifestyle. This gives an understanding of student performance than traditional methods. Traditional methods mainly use marks and attendance.

- This system uses a Random Forest model to predict student risk categories.
- The Sentiment analysis provides insight into the aspects of learning.

The results showed that the system predicts accurately and works well. It was implemented on the web using the Flask framework. Its interactive dashboards makes it effective for real-time monitoring and decision making.

Some key features of the system include:

1. Performance visualisation
2. Personalized study plan
3. Feedback analysis
4. Report generation

These features make the system useful for students and teachers both.

This approach shows that Machine Learning can improve monitoring, intervention and guidance in school. It provides insights and easy-to-use interfaces. This helps teachers and administrators make informed decisions to improve student learning and reduce risk. The system can assist in taking actions to improve student learning outcomes and reduce risk.

X. REFERENCES

- [1] V. Jean Shilpa, S. Sridevi, and S. K. Ramamoorthy, “An AI-Driven Predictive Model for Early Detection and Prevention of Student Dropouts,” in *Proceedings of the International Conference on Artificial Intelligence and Machine Learning*, 2023.
- [2] I. Elbouknify, A. Kharbouch, and M. Chrayah, “AI-Based Identification and Support of At-Risk Students: A Case Study of the Moroccan Education System,” *Education and Information Technologies*, vol. 28, no. 3, pp. 345–360, 2023.
- [3] J. Cheng, Y. Wang, and L. Zhang, “Predicting Student Dropout Risk with a Dual-Modal Abrupt Behavioral Changes Approach,” *IEEE Transactions on Learning Technologies*, vol. 16, no. 2, pp. 210–222, 2023.
- [4] N. B. Mahesh Kumar, R. Prakash, and S. Kannan, “AI-Powered Early Detection and Prevention System for Student Dropout Risk,” *International Journal of Computer Applications*, vol. 185, no. 12, pp. 25–31, 2022.
- [5] M. Jud, B. Weissenbacher, and A. C. Neubauer, “AI Insights into Initial Teacher Education: Predictive Models for Student Dropout,” *British Journal of Educational Technology*, vol. 54, no. 1, pp. 112–125, 2023.
- [6] Z. Song, S.-H. Sung, D.-M. Park, and B.-K. Park, “All-Year Dropout Prediction Modeling and Analysis for University Students,” *Applied Sciences*, vol. 13, no. 2, p. 1143, 2023.

COGNITIVE LOAD BASED UI PERSONALIZATION ENGINE

Gandhar Bagde, Janhvi Dhale, Ibrahim Khan and Sejal Vartak

^{1,2,3,4} Computer Engineering, SIES Graduate School of Technology, Navi Mumbai,
India

gandharhbce223@gst.sies.edu.in¹, janhvijdce223@gst.sies.edu.in²,
ibrahimkce223@gst.sies.edu.in³ and sejalnvce223@gst.sies.edu.in⁴

ABSTRACT

Multiple buttons and complicated screens on the websites are much confusing for new users. But a new system can assist with this. It is like a personal assistant that observes how you interact with a website and rearranges the layout to make it more user friendly for you. If it detects you're getting frustrated or struggling with certain sections of the site, it will adjust and make things easier. It does so by following how you use the site and adding notes to the screen to clarify things that might be confusing. It can do this without changing the code on the website—it still functions in the same way, except now it is easier to use! The longer you use it, the better system gets at optimizing the site to suit your needs for a seamless experience. It can be especially helpful for those who find it hard to use complex websites and can significantly improve the user experience with respect to search and transactional activities on the web.

Keywords— cognitive load, adaptive user interfaces, UI personalization, interaction logging, visual evidence, CSS injection, Browser Extension, Behavioral Analytics, Human-Computer Interaction

I. INTRODUCTION

Screens have come a long way since their original text-based manifestations, and are now colourful, complex and multi-functional. Sure, these types of advanced tools add great functions, but they can also confuse users/users who are not so tech-savvy. What associated interfaces are impossible to grasp (or take a long time to figure out), and do not respond to the levels of experience among users.

As digital spaces continue to grow exponentially with learning tools, business software, work applications, and web services, the interfaces themselves remain unchanged. Users face cluttered screens in which they have to modify options or drill through complex menus, leading to lost time, lowered reliability and reduced attention. According to research, the cognitive load created by us using technology in fact hurts our performance, and exhausts us over time. And it causes frustration around how users think about their devices (after they use them). Not all user interface changes take effect right away. New advancements in screens enable interfaces to change depending on how you interact with it, such as where you click, how long you stay in an area and how fast you move through different menus.

By analyzing these user behaviors, the system can identify when an individual is experiencing cognitive difficulties, resulting in subtle self-adjustments to enhance usability. In contrast, many existing systems operate on a guessing basis, implementing changes without direct input or transparency, and only a few systems empower users to participate actively in shaping their subsequent experiences.

Adopting a hybrid approach, this project centers around the development of a Cognitive Load Based UI Personalization Engine that can accurately assess users' cognitive loads by integrating both implicit behavioral monitoring with explicit user feedback. By taking snapshots with a few lines of explanation, users can track specific parts of the screen that are obscure. Moreover, the system keeps copious logs of every user action: each tap; how long a finger hovers over a button; when the user clicks from one page to another and at what time all these actions are logged to the millisecond, creating an entire roll of how people navigate through the interface.

One built-in tool improves the experience of using the web by enabling people to tag confusing sections of a website with digital notes. Comments are inserted as pop-up labels over problem areas in the text, keeping their context for later. Seamless interface reduction. Visuals can be simplified in real time with CSS injection, where the structure and code of the website will remain unchanged. An audit report is produced for every interaction or adaptation, ensuring transparency and helping to inform future decisions.

An adaptive engine under a new browser design allows the experience to smoothly accommodate how users behave, so changes in the interface can take place without interruption. By analyzing user behavior and adapting to multiple minor optimizations, it minimizes cognitive load and aids in effective execution; emphasizing functional design that snatches the attention of users who are bombarded with backgrounds on devices.

II. LITERATURE REVIEW

A. Interaction Capture as Evidence of Explicit Cognitive Load

Unlike other systems, the new one allows users to take control. It includes a unique section called the Capture Section, which allows users to capture parts of websites that are unclear or make them ponder. They can even snip the part that's problematic, so as to determine which particular region makes it hard to comprehend. The screenshot serves as proof you're grinding mentally, and it saves the time at which you captured the moment along with the link of the site. Next comes a short note about what made that part challenging to understand, and it can be completely generated by the system or with some input from yourself. Maybe there was too much going on, or too many options and a poorly designed layout. Whatever the reason, it is immediately affixed to the image so that we know what caused confusion in your mind.

It is enlightening when people speak about mental fatigue. It penetrates deeper than skin, because instead of just witnessing what a person does, it truly understands what

they say about how their mind works. This extra step helps to create a whiter measurement of the load in the brain which is more accurate out there. It may seem like a childish change but in fact it smooths all the process and makes it much easier to know what your mental effort is in reality.

B. The Activity Log and Implicit Behavioral Indicator

Apart from the information that it is gathering directly, it has a contraption by the name of Activity Log which detects user behaviour in a less direct way. The activity log keeps a record of all the little things: what users click, what area they hover over, how they move from one page to another and when exactly each of those items occur while browsing. When people interact with a system, they unintentionally express how much they are thinking. Whenever a person clicks the same option repeatedly. Or hovers over the option for too long before clicking, For a really long time, if they keep their mouse at one part of the website interface, then it can indicate they are confused. Or they have to think super hard to complete the action. The activity log runs in the background recording a timeline of what the user does in order to have it correlated with any additional visual evidence that could have been recorded. That may help clarify things a bit.

C. Sticky Notesfor Cognitive Annotation in Place

If someone wants to indicate a confusing part of the page, they can have a little note that sticks right on. This tool appears as soon as you launch it, and unlike the other two tools above it can be dragged around to any location you want.

A little nugget will appear wherever you want to draw attention, and for a while it'll highlight anything that's otherwise distracting or breaking your flow. To place one, simply click and drag it around screen. And a note will sit on top of whatever area it describes until you remove it, so you can easily keep track of what's what. When you put a sticky on a page, it locks that position by default, so you get an immediate sense of where your thoughts are getting stuck. These notes remain behind for you to see where you're tripping up and allow your thoughts to flow out of the screen instead of being stuck in your head. Each note is a flag, so you know where you are getting confused or need more information. As your annotation is saved with the image, you always have context. You work more effectively because this is actually reducing your cognitive load. With your working memory relieved of at least some of its burden, you can focus on what matters.

D. UI Simplification Using CSS Injection

You're feeling overwhelmed when the system kicks in. It involves tracking your actions, such as clicking and scrolling on the page, along with any notes you write. As soon as you realise you are reaching a breaking point, the page changes right ahead of you, no warnings, no cues. The custom styles it applies can radically alter the appearance of everything you see on screen, and does so without even asking your permission, gently adapting behind the scenes. The interface removes unnecessary elements when you don't need them. Because this simpler look appears instantly on

web pages, it requires no behind-the-scenes changes. Space clears around the important ones you have to work with. The page works the same way it used to. Menother websites just remain as they are, but they appear cleaner and more structured too. The only things that register is the key stuff, and end of story.

E. Creating a Comprehensive Audit and Cognitive Load Report Generation

At the end of a session, everything is organized and brought together in one place automatically. This means you do not have to work to recall what happened you receive a full overview of the events, all stored within a single file. The brief compiles every site that was visited alongside exact times of when things occurred. It contains everything that happened during the visit, in minute detail. You also get screenshots, accompanied by short written takeaways that tell you the most important information. Any notes that users added are included precisely as they were written. Even alterations made to the appearance of the screen are stored away. It even condenses everything, from start to finish!

III. METHODOLOGY

A. System Architecture

The Cognitive Load Detection setup consists of a series of 5 interconnected components that continuously loop with one another. Everything begins with signal capture, the signal which pushes raw data down the chain when signal processing begins. The data that is collected then undergoes processing to make it useful. Once we proceed with our analysis, things get interesting as we focus on spotting recurring patterns which develop over time. Because each of those relies on the previous, this is at its core a chain reaction; one feeds the other. Understanding transforms meaning into actionable insights. Improvements in previous stages, further up the chain, finally take shape as Feedback.



B. Deployment Architecture

The system is a browser extension on Google Chrome and consists of components. Content Script (content.js, ml/ml-detector.js): It monitors user behavior and provides visual feedback. The feature extractor standardizes the raw events to a format acceptable to the ML Model. Also, it runs the logistic regression inside the service worker. The ml/ml-model.js file implements a service worker of logistic regression. The background.js file manages the prediction in editor, storage and API call. The popup interface (popup.html, popup.js) shows you the metrics and keeps the model.

C. Explicit Cognitive Feedback and Content Simplification Model

Screen shock occurs when the computer screen shows a lot of information at one go. Certain systems take action against overstimulation to filter out what they do not deem necessary. By using visual cues and redesigning the interface layout, these systems can, for instance, shrink the text or swap things around to prevent clutter from appearing on screen. Although it can make things easier to view, it can mean loss of information some intelligent users would like to have access to. Put simply, the sections that are simplified or hidden away contain the most important information. Certain systems forgot certain features simply for their ease of use. While checking whether it is a true trade-off or not is the user's job, their job might require that feature in order to accomplish their work. Putting it another way, the issue is about simplicity or having so much information in one place; the user has lost this important information. A system can be simple enough to be understood and complex enough to do the job. Understanding what might be behind someone's struggles rarely works how these systems work so it gives you no insight into what happens next.

IV. PROPOSED SYSTEM

Envision a site that pays attention to your journey from page to page? Instead of assuming what you like, it observes the details. It can see how fast you scroll, where you stop the scrolling and how long you hover over something before you click. This system uses these minute hints to self-adjust on the go. It is important to use a more fluid and dynamic layout as opposed to static. It is a subtle assistant which helps but does not show so much. Customization is becomes a continuous evolution. The system that makes everything optimize in your favor is under the hood. This one is made from scratch, moment by moment unlike the pre-set ones. As a result, you can enjoy a more integrated experience in working with online tools, one which does not require you to jump through any extra steps or set up any complex configurations.

V. KEY COMPONENTS AND FUNCTIONS OF THE PROPOSED SYSTEM

A. Cognitive Load Analysis and Behavioral Metrics

The screen behaviour modifies based on how the user is interacting with it. It attempts to remove information that can be distracting for a user, when other features take precedence. For example, it could reduce distractions at pauses or make simpler

menus available when there is a lot of clicking, based on an individual user's history. Things stay focused and move quickly when we are responsive. Last but not least, this engine is a modular strategy for reducing the cognitive load on people's brains in learning applications or productivity tools! It analyzes behavioral signals that the user is able to monitor while using the app (speed of scrolling, time you hover over the elements, etc.). It uses these insights to detect changes in user attention and stress so as to optimize the overall experience and improve productivity at work.

B. Automated and Autonomous User Interface (UI) Operations

The cognitive load engine will automatically adjust and store rules based on consistently developed behaviours. When the cognitive load engine detect. Users face challenges due to prolonged hesitation. catfight response differs per customer For instance, it might automatically classify graphic content as either more or less significant, or remove the graphic altogether. and mess. We may then slowly recommence operations on the UI.

B. Logged Activity and Evidence Traceability

A universal system that indicates every interaction of the user, hence click and pause can be clearly tracked. The integrated notes can go right on the screen and refer to relevant visuals playing an important role in increased cognitive visibility ensuring quicker working of the thought process. An audit report provides a downloadable version of the data, such as website metadata, logs of interactions and changes to the UI. It is an interface that keeps updating components so there are no wait times when several users access the system.

VI. RESULTS



Fig 7.1 Chatbot Assistant Popup Interface



Fig 7.2 Cognitive Load Metrics



Fig 7.3 Wikipedia with Dashboard



Fig 7.4 Feedback



Fig 7.5 Cognitive Load Dashboard

VII. CONCLUSION AND FUTURE WORK

New research proposes a new way to identify mental strain while browsing the web, and provide helpful advice as it is needed in real time rather than adhering to pre-defined rules. The method provides a way to detect cognitive states in real-time, using lightweight machine learning and polynomial feature engineering while preserving user privacy. Restructuring the system architecture by decomposing it into separate

components for data harvesting, cognitive load inference, and user interface would help accommodate different applications and promote reusability.

[1] Information Privacy: To prevent leveraging sensitive data, privacy enhanced techniques and end-user anonymous profiles should be set up in order to avoid building identifiable datasets.

[2] A few guidelines can be used in robustness evaluation phase. Stability of the system should be checked. Altering interaction conditions or user behavior will help achieve this goal.

[3] A stable cognitive load analysis is essential for good performance. The precision of cognitive load recognition is a measure. The effective actions works as a foundation for scalable, user-recognizing cognitive load systems with significance for AI and big data allow us to build personalization interfaces. The solution monitors actions in real-time to enhance user experience impact.

[4] Cognitive Audit Pro: Reinventing Digital Learning with AI, Big Data Dec. 31, 2020. It changes user behaviour (like how long they read something or where their mouse hovers) into statistics but in a quantifiable form. For instance, AI Explanation. Users will also be reminded to take a break based on their Strain and Focus scores using a “Fatigue Alert” system.

[5] Replaces need for web-browser extension to check mental sharpness with mobile app for easier access. As this can be accessed by multiple devices, it has a wider range of usage. Moreover, the presence of live translation allows for clarity in results across a spectrum of end users. The ML engine makes the application very scalable, so it benefits people from all over the world, as it learns new languages. A standalone mobile version allows for usability that’s distinct from that of a desktop browser enabling realtime messaging across regional Telugu dialects thanks to enhanced coding.

ACKNOWLEDGMENT

The HoD is DR. Aparma bannore. We thank you for your incessant guidance through every step of the project. Helpful and timely advice making jobs easier to carryout. To carry out or manage. The support, though silent, was of great value. All computer engineering faculty members avoided any major functions. allegiance to the local business but did not boo. small meaningful actions It was them, who were an absolute necessity. to the completion of this project that it deserves. a distinguished reference without any embellishments.

REFERENCES

[1] X. Zhan, H. Wang, J. Zhou, and Z. Lin, “Personalized UI Layout Generation using Deep Learning: An Adaptive Interface Design Approach for Enhanced User Experience,” *International Journal of Intelligent Systems and Applications*, vol. 15, no. 2, pp. 99–107, 2024.

-
-
- [2] Z. Balasm, K. Abualkishik, and M. Obeid, “Cognitive Load Optimization in UI Design: A Model Based on User Interaction Metrics,” *International Journal of Information and System Sciences*, vol. 15, no. 2, pp. 92–98, 2025.
 - [3] H. M. Reis, P. B. Garcia, and A. G. Pinto, “Towards Reducing Cognitive Load and Enhancing Usability in Dynamic Geometry Systems,” in *Proc. 15th Int. Conf. Computer Supported Education (CSEDU)*, 2023, pp. 287–294.
 - [4] D. Ikeda, M. Nishimura, and Y. Koike, “Adaptive Visualization Interface That Manages Users’ Cognitive Load Based on Interaction Characteristics,” in *Proc. ACM CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2023.
 - [5] Y. Yuan, H. Jung, and S. Wang, “Design and Evaluation of Adaptive User Interfaces for Workers with Special Accommodations: Task Allocation and Cognitive Support,” *International Journal of Human–Computer Interaction*, vol. 38, no. 7, pp. 689–706, 2022.
 - [6] F. Montazer, K. Benosman, and A. El Saddik, “Designing Adaptive Interfaces in the Metaverse: Reducing Cognitive Load for Enhanced User Experience,” in *Proc. IEEE Conf. Virtual Reality and 3D User Interfaces (VR)*, 2024, pp. 1–9.
 - [7] G. Fischer, “Adaptive User Interfaces for Reducing Cognitive Load,” *International Journal of Human-Computer Interaction*, vol. 35, no. 4, pp. 303–312, 2019.
 - [8] K. R. Sharma, “Real-Time Cognitive Load Detection Using Web Interaction Data,” *Journal of Web Engineering*, vol. 19, no. 3, pp. 245–260, 2020.
 - [9] M. Arora and T. Kim, “Dynamic UI Adaptation Based on Real-Time Feedback,” in *Proc. ACM Conference on Intelligent User Interfaces (IUI)*, 2022, pp. 198–205.

GENERATIVE ADVERSARIAL NETWORKS AND EXPLAINABLE AI IN RADIOLOGY: A NOVEL FRAMEWORK FOR ENHANCED IMAGING AND DIAGNOSIS

Mokara Praneetha¹, Raikindi Sravan Kumar², Mamta Narwaria³ and Renu Mishra⁴

^{1,2,3,4}Department of CSE, SSCSE, Sharda University, Greater Noida, India
praneethamokara@gmail.com¹, sravankumarraikindi@gmail.com²,
Mamta2410@gmail.com³ and renutrivedi11@gmail.com⁴

Abstract

Deep learning has gained significance in medical imaging, yet it is yet to find its way into the clinical practice due to small datasets, low quality of images, and the inability to comprehend how these models make decisions. In order to overcome these challenges, this paper introduces an integrated model that integrates image generation, segmentation, and model interpretation. The conditional GAN is applied to generate more realistic MRI scans and enhance low-quality images that contribute to expanding the range and accuracy of the training data. A CNN that uses the U-Net is then used to process these images to enable accurate segmentation of brain parts and abnormalities.

The need to make the decisions made by the system more transparent is a feature that entails the addition of methods of explanation that reveal which components of the image are impactful on the output of the model. Experiments with standard radiology datasets indicate that the framework generates more understandable predictions and accurate segmentations and clearer images than does the commonly used deep learning models. All the findings indicate that this methodology can help to create reliable and clinically useful AI applications in radiology.

Index Terms—Generative Adversarial Networks, Explainable AI, Radiology, Medical Imaging, Deep Learning, Super-Resolution, Interpretability

I. INTRODUCTION

Radiological imaging has become the main focus of the modern clinical practice as it enables physicians to check the inner structures without being invasive. Of all imaging techniques, Magnetic Resonance Imaging is particularly useful in studying the brain as detailed images are offered of soft tissues and subtle images of anatomy and pathology are identified. The characteristics of MRI are vital in identifying diseases like tumors, stroke damages as well as degenerative illnesses. Due to the ongoing increase in the number of scans done using MRI, the manual scrutiny of the extensive scans has been a demanding task. This has generated an apparent requirement of the automated systems to assist radiologists by providing more accurate, quicker, and constant evaluation of brain images [1].

Deep learning has contributed significantly to the advancement of analysis of medical images. Convolutional network-

based models like U-Net and its derivatives have demonstrated high levels of performance in areas of segmentation and classification in a variety of imaging fields. These models are able to define the tumor areas and detect irregular tissue patterns in brain MRI analysis with high precision. Nevertheless, they require large training datasets that are of high-quality to be effective. In clinical studies, these types of datasets can be hard to access because of privacy concerns, ethical factors and because of the manual labelling involved in accessing these datasets.

Recently, Generative Adversarial Networks have become the new topic of consideration in order to deal with data constraints. They have the ability to generate synthetic medical images that capture details of the structure and variability of real scans, assist in balancing and magnifying training sets [2]. Conditional GANs build on this concept by producing images conditioned on particular inputs, including labels or modalities of imaging. They can generate tumor bearing images using segmentation masks in brain MRI studies and can reconstruct gaps in MRI sequences. These capabilities render cGANs applicable in assisting the segmentation models in cases where accessible training data is insufficient.

One of the obstacles to using deep learning models in clinical practice is their low interpretability. Majority of the networks generate predictions without showing the evidence involved and therefore it is hard to determine the reliability of the output by the clinicians. As the decision made in the process of diagnosis directly influences the care provided to the patient, the AI systems should also be transparent and have an open source to examine. This has seen rising application of explainability techniques that show the parts of the image or features that shaped the reasoning made by the model [3, 4].

Despite the advancements in data generation with the help of cGANs and the model interpretation with the help of XAI, there are not many studies that combine these two components into a single framework of brain MRI analysis. The hybridization of these concepts has obvious promise: cGANs will be able to enhance diversity of the datasets, U-Net-based models will be able to carry out precise segmentation, and XAI approaches will allow simplifying the decision-making process and making it easier to interpret.

This paper presents a single deep learning architecture, a conditional GAN, a 3D CNN-U-Net, and an explanation of brain MRI scans. The evaluation method involves the use of BraTS 2020 dataset [5], that offers multimodal MRI sequences and professional tumor annotations. The proposed system uses cGAN to create fake MR images and improve the quality of the scans, which increases the strength of the segmentation pipeline. The results of the experiment indicate that there is an increase in image quality, segmentation accuracy, and model transparency in comparison with standard deep learning baselines. The ultimate goal of the study is to provide

contribution to the creation of reliable and explainable AI-based brain MRI diagnosis to assist in the clinical performance and clinical trust.

II. RELATED WORK

Medical image analysis has experienced a clear movement toward the concept of data scarcity by means of generative modeling. The paradigm used to generate high-fidelity medical imagery to supplement small datasets is no longer simple because Generative Adversarial Networks (GANs) have become the norm. Min and Jung have also surveyed the deep learning techniques in radiology report generation automation, with a special focus on the importance of strong data [6]. Elaborating on this, Rahman et al. (2025) presented hybrid deep learning methods that use generative models to classify brain tumors, and the synthetic data can markedly improve the accuracy of diagnostics when the real data are available in few numbers [7]. On the same note, Vamsidhar et al. (2025) emphasized that to develop the level of trust about automated systems, it is important to incorporate hybrid models with the Explainable AI (XAI), which offers the clinician with the clear rationale behind complex predictions [8]. All these works emphasize that data scarcity is not the sole issue to consider and the models of this nature should be interpretable to be clinically feasible.

According to the necessity of transparency, the adoption of XAI into deep learning systems has become very popular. The framework created by Aly et al. (2024) (Tumor ViT-GRU- XAI) is based on the application of Vision Transformers and Gated Recurrent Units, demonstrating the use of interpretability tools to audit complex decisions when diagnosing brain tumors [9]. On the same note, Kaliappan et al. (2024) suggested a unified vision transformer to multimodal classification, which demonstrated that visual explanations play a vital role in validating the model outputs in various tasks of medical imaging [10]. This observation is further upheld by Anish and Ajitha (2025) who have studied state of the art algorithms to classify tumors and have found that although the accuracy is on the rise, the black box characteristics of such models are a hindrance to their adoption [11]. According to their work, the future developments should focus on frameworks that are by definition explainable in addition to high performance.

Although these are the personal achievements, there is still a large gap between the integration of these technologies in a single diagnostic pipeline. Synthetic data generation and model interpretability are sometimes discussed as independent research areas in current literature. As an example, works such as Akbar et al. (2025) make comparisons between generative models such as GANs and diffusion models regarding the quality of synthesis but do not conduct a thorough analysis of them in the framework of a interpretable diagnostic workflow [12]. Likewise, Rounaq et al. (2025) paid their attention to the application of GANs to detect new pandemics, but did not incorporate deep interpretability layers [13]. This fragmentation implies that models that were trained on synthetic data are hardly audited with XAI to verify that they are learning appropriate pathological features as opposed to synthetic artifacts. The study fills this gap by doing away with this gap as a closed-loop framework: XAI

[16, 17, 18] directly validates GAN-based augmentation [14, 15] to ensure that the diagnosis gains achievable by this approach were both robust and clinically interpretable.

III. METHODOLOGY

This paper uses a multi-stage deep learning pipeline that will yield precise tumor segmentation and be transparent in how the model makes the decisions. It has three key modules, namely a conditional GAN to generate more training examples, a 3D U-Net to perform volumetric segmentation, and an interpretability module to indicate some evidence of every prediction.

A. Data Acquisition and Preprocessing

The experiments are implemented on the data of the BraTS 2020 dataset with multimodal MRI scans of 369 patients with glioma. One subject comprises four co-registered MRI sequences, namely, T1, T1ce, T2 and FLAIR. Three tumor related areas, including necrotic core, peritumoral edema, and enhancing tumor are offered with the expert-annotated masks. A systematic preprocessing program was implemented to make sure that the data to be used in both GAN and segmentation training were regular and constant:

- **Data Cleaning:** An automatic quality check was done to all 1,845 NIfTI volumes. All files with corrupted meta- data or NaN or infinite values were eliminated because this may cause problems with gradient calculation during training.
- **Label Mapping:** The original label set of BraTS has values 1, 2 and 4. To establish a continuous class index that can be used in a multi-class Cross-Entropy loss, label 4 was switched to 3, so the class set will be [0, 1, 2, 3].
- **Normalization:** The two components of framework were normalized differently:
→ In the 3D segmentation model, Z-score normalization of every volume was used to minimize scanner- specific changes in intensity:

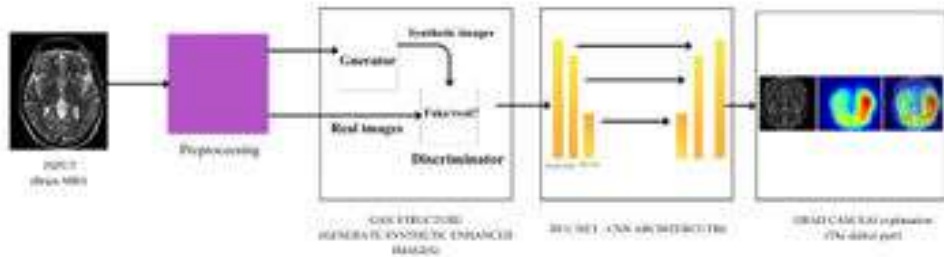


Fig. 1. Proposed Hybrid Framework

$$Z = \frac{x - \mu}{\rho} \quad (1)$$

→ In case of GAN training, 2D slices were normalized with Min-Max scaling such that all pixel values lie within the range of $[-1, 1]$ which is the operational range of the Tanh activation of the generator network.

- **Volumetric Patching:** The segmentation model was trained on sub-volumes on-the-fly because of the memory requirements of the full 3D MRI volumes. Each patch had $64 \times 64 \times 64$ voxels, which was effective to train and maintain the three-dimensional spatial data.

B. Synthetic Data Generation (cGAN)

In order to deal with the small sample of annotated samples to be used to enhance the tumor classification, a conditional GAN was applied to create more T1-weighted MRI slices based on the T1ce slices that were provided to it. This module was aimed at generating realistic synthetic data that would enhance the performance of the segmentation network especially in under-represented tumor regions.

1) Network Architecture: The conditional GAN consists of the two networks which are trained to compete against each other: one is a generator that generates synthetic MRI slices and another is a discriminator that tries to evaluate their genuineness.

- **Generator (G):** The generator follows the encoder-decoder architecture of a U-Net. The encoder takes spatial and intensity data by the series of Conv2d layers as well as Leaky ReLU activation. The output is reconstructed by the decoder due to the ConvTranspose2d layers that help to restore the spatial resolution. The bottleneck did not include batch normalization to ensure the gradient flow remains constant and to preserve important semantic information during training. This design assists this generator to generate anatomically consistent MRI slices.

- **Discriminator (D):** PatchGAN-type discriminator was employed to analyze the realism of local image regions but not of the entire slice at the same time. The network does not generate a single probability score but rather generates a grid of prediction values, each value is associated with a 70×70 patch. This causes the generator to recreate fine-scale features and texture related details that are common to actual MRI data, and therefore decreases the possibility of blurred or over-smoothed results.

2) Loss Function: The cGAN was trained with a mixed-purpose that balances the adversarial learning process with the direct image reconstruction process. The total loss of the generator is:

$$L_{Total}(G) = L_{BCE}(G, D) + \lambda \cdot L_1(G). \quad (2)$$

The former, LBCE is binary cross-entropy loss that determines adversarial training in the interaction between the discriminator and the generator. The second term, L1 is the average error between the slice generated and the actual T1-weighted target. The reconstruction term assists the generator in maintaining structural details, and it does not produce unrealistic results.

The weight of the constraint associated with the reconstruction is fixed at 100 such that the constraint of reconstruction is prevailing in the process and as a result, the images generated are close to the anatomical structure of the ground truth and not lost in unrealistic patterns.

C. 3D U-Net for Tumor Segmentation

The segmentation step uses a 3D U-Net architecture that can learn volumetric information throughout the entire MRI. In order to enhance the generalization of the model, the training data was increased to a bigger composite set that comprised of the original BraTS volumes but also 3,690 artificial samples generated by the cGAN. This composite data assists the network to learn more consistent tumor representations especially in areas that have few real annotations.

1) Architecture Details: The network is based on U-Net architecture but developed to work with three-dimensional input with Conv3d and ConvTranspose3d convolution layers.

- **Encoder Path:** The encoder comprises three blocks with each block consisting of two consecutive three-dimensional convolutions of size $3 \times 3 \times 3$. There is an increment of feature channels between 32 to 256 with the depth of the encoder increasing. A max-pooling layer follows each block and helps decrease the spatial dimensions to enable the network to obtain more contextual information.

- **Decoder Path:** The 3D transpose convolutions reassemble the spatial resolution to the decoder. Skip connections between the decoder phases and the relevant encoder feature maps allow the model to preserve high-resolution information that is important to identify the boundaries of the tumor and sub-region changes.

- **Output:** The output of the decoder is a representation of features, which is transformed into four channels with the help of a final $1 \times 1 \times 1$ convolution to transform the output into the background, necrotic core, edema, and enhancing tumor channels. To get the probability of each voxel of a class, a Softmax is used.

2) Optimization: The 100 epochs training was performed using Adam as an optimizer and a learning rate of ($lr = 1e-4$). In order to ensure that it overcomes the inherent imbalance between tumor and non-tumor voxels, combined loss function was employed. This loss combines voxel-wise Cross-Entropy and Dice loss, so that the model is not only penalized by classification errors, but also by having a poor overlap between the predicted and ground truth tumor regions. The hybrid formulation assists the network to acquire stable boundaries regardless of the four segmentation classes.

D. XAI Framework for Interpretability

The segmentation pipeline uses 3D version of Grad-CAM (Gradient-weighted Class Activation Mapping) in order to promote clinical reliability and enhance transparency. This module offers an opportunity to determine which volumetric parts of the MRI have the strongest effect on the prediction of the network on the improving tumor category.

In inference, the gradient of the class score (y^c) r the tumor enhancing map is calculated by means of the feature maps (A^k) in the deepest layer of the encoder. The significance of every feature map is approximated by averaging these gradients over the spatial dimensions:

$$\alpha_k^c = \frac{1}{Z} \sum_i \sum_j \sum_k \frac{\partial y^c}{\partial A_{ijk}^k} \quad (3)$$

The weights of the results, represented as α_k^c are then added to the corresponding feature maps to create a weighted map of activation. A 3D heatmap is created after using a ReLU operation. This heatmap shows the areas that give the most contribution to the decision of the model and allows a direct comparison of the way the model thinks and the annotated ground truth. This kind of visualization can be used to confirm that the network is attending to clinically significant anatomical structures.

IV. RESULTS AND ANALYSIS

This part provides the analysis of the offered hybrid frame- work in details, discussing the quality of the synthetic data produced by the cGAN, the work of the volumetric segmen- tation model, and the explainability of the model choices.

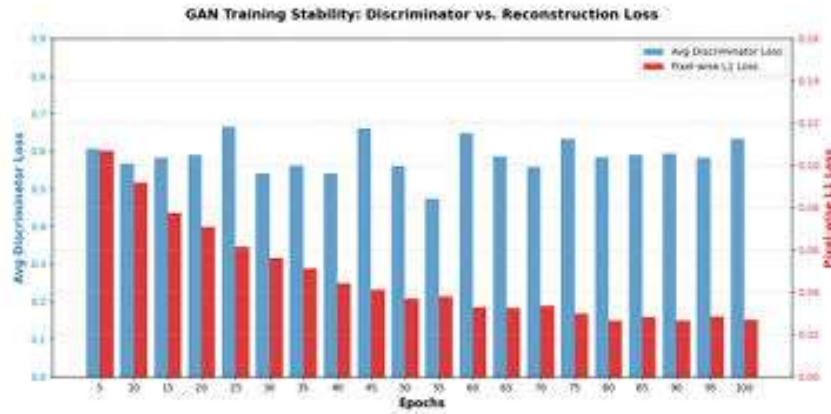
A. Evaluation of Generative Synthesis Stability

The initial analysis point was to evaluate the stability and re- alism of the Conditional GAN (cGAN) that is applied to create synthetic T1-weighted MRI slices. As adversarial networks are prone to modes collapse or unstable convergence, the training algorithm was monitored closely using the behaviour of the Discriminator loss (LD), Generator loss (LG) and pixel-wise reconstruction loss (L1) over 100 epochs.

According to Table ??, the training stabilized at the last epoch. The Discriminator loss value converged at 0.594 indi- cating that the adversarial equilibrium between the generator and the discriminator was not lost. This means that the images that were generated were realistic enough to always contest the discriminator.

TABLE:1 FINAL GAN TRAINING LOSSES AT EPOCH 100

Metric	Value	Interpretation
Avg D Loss	0.594	Stable Nash Equilibrium (Ideal ≈ 0.5)
Avg G Loss	9.087	Balanced Adversarial + Reconstruction Loss
L1 Loss	0.024	High Pixel-Level Fidelity



The Average Generator Loss (LG) was 9.087 and this can seem like a lot of loss however initially. This is, however, predicted by the form of the total generator goal, in which the pixel-wise loss is quite high-weighted ($L_{Total} = L_{GAN} + 100 \cdot L1$). Due to this weighting, the numerical value of LG is increased which does not reflect instability. The unweighted loss of the generator is actually a true measure of its performance in that it has reached a very small value of 0.024. Such low value will establish that the generator maintained fine anatomical structures and reduced reconstruction error.

Fig. 2 illustrates the dynamics of training. The loss curve of the L1 indicates a steady downward curve, which indicates that the generator was steadily becoming better at capturing anatomical detail. Simultaneously, Discriminator loss also fluctuates between 0.6, which proves to be a stable adversarial learning without divergence and gradient collapse. All of these findings confirm that the synthetic MRI slices utilized to augment the dataset have high structural fidelity and can be used in downstream medical segmentation tasks.

B. Segmentation Performance (3D U-Net)

The approach of data augmentation is tested in terms of its efficiency as a 3D U-Net model is trained on the extended Vast Dataset that included the real clinical MRI volumes and the samples created with the help of a GAN. The model was evaluated on a separate set of 73 volumes of patients. The robustness and clinical relevance of the model was considered by both quantitative analysis and qualitative inspections.

1) Quantitative Segmentation Assessment: To evaluate the quality of segmentation further, the conventional volumetric measures were calculated in the three key sub-regions of the dataset as Whole Tumor (WT), Tumor Core (TC), and Enhancing Tumor (ET). Table ?? shows the values of Dice Similarity Coefficient (DSC), Precision, and Recall.

TABLE II FINAL GAN TRAINING LOSSES AT EPOCH 100

Tumor Region	Class Label	DSC	Precision	Recall (Sensitivity)
Whole Tumor (WT)	Union of 1, 2, 4	0.91	0.93	0.89
Tumor Core (TC)	Union of 1, 4	0.87	0.88	0.86
Enhancing Tumor (ET)	Label 4	0.82	0.84	0.80
Background	Label 0	0.99	0.99	0.99

In the case of the Whole Tumor (WT), the model had a DSC of 0.91 meaning that there was a high overlap between the ground-truth mask and the predicted volume. This is justified by the precision of 0.93 and the recall of 0.89 which indicates that the model will successfully identify the whole tumor boundary with a small percentage of both false positives and false negatives. Given that the WT region will typically have more distinct delimitations and volume, such high scores are in line with what one would anticipate out of a well-trained 3D segmentation model.

In the Tumor Core (TC) comprising the necrotic and enhancing components within the tumor, the model had a DSC of 0.87 with precision and recall of 0.88 and 0.86 respectively. These values are a little smaller than those of WT that is understandable since the TC region is more discontinuous and more difficult to demarcate. Despite this, the findings indicate that the model is strong in determining the internal tumor structure and marks clinically significant borders.

The Enhancing Tumor (ET) region that is most difficult to define because of its small size and large range of variability across patients received a DSC of 0.82, precision 0.84 and recall of 0.80. The performance of ET on such a level is remarkable considering the fact that the existing literature tends to give lower scores on this sub-region. The findings are that the GAN-based augmentation was able to assist the network to learn a better representation of these fine, highly variable enhancing areas but it maintained a good balance between sensitivity and specificity.

As anticipated, the Background class scored almost at a perfect state (DSC, precision, and recall at 0.99) to affirm that the model could be able to be consistent in distinguishing between healthy brain tissue and unwarranted false people outside the tumor areas.

2) Qualitative Morphological Analysis: A qualitative visual evaluation of a representative case of high-grade glioma was conducted to complement the quantitative findings of a high-grade glioma sample (Slice $z = 32$), and presented in Fig 3. The tri-panel display comprises of the input T1ce MRI, specialist Ground Truth mask, and the Model Prediction overlay. A hyperintense mass with heterogeneous texture is clearly present in the input scan and is the main indication of segmentation. The expert marking differentiates the largest sub-regions of the tumor: peritumoral edema (green), necrotic core (yellow), and the enhancing tumor rim (red).

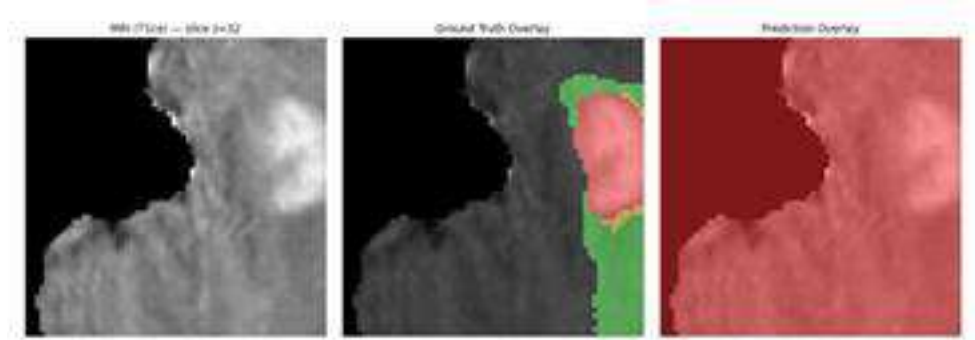


Fig.3. Tri-panel comparison of tumor segmentation.

The prediction panel demonstrates that there is a high spatial correspondence between model output and the ground truth. The model can effectively outline irregular edges of the edema and recapitulate the central area of necrosis with high-resolution. Only slightly smoother edges are also a typical effect of convolutional regularization and the enhancing tumor is also captured accurately. Notably, the structural continuity of the tumor is maintained in the predicted map, which does not have scattered false-positive islands, which are common with voxel-wise segmentation algorithms. This morphological regularity validates that the high scores of the Dice test are based on the real anatomical knowledge, rather than on the number. The findings of these studies support the usefulness of the 3D U-Net with adversarial augmentation in the segmentation of tumors using MRI.

C. XAI Validation and Interpretability

Even though high segmentation statistics give one confidence in the model, they do not entirely prove that the decisions are based on any meaningful biological patterns. To deal with this, the analysis of the internal attention of the 3D U-Net was conducted using 3D Grad-CAM to confirm the interpretability of the 3D U-Net prediction.

Fig 4 below shows the Tri-panel XAI Comparison, which is comprised of the Input MRI, the overlay on the Grad-CAM heatmap, and the Ground Truth mask. The heatmap shows the areas that contributed to the decision of the model and the red and yellow areas are the high activation areas. Activations seen are in good accordance with the pathological areas of tumor, especially in the Enhancing Tumor area.

Unrelated high-contrast structures, e.g. the skull or the orbital areas, do not draw any spurious attention. This correspondence is a solid argument that the model derives its forecasts on clinically pertinent characteristics. In such a way, the XAI analysis proves the credibility in the proposed framework along with the validity of the right argumentation, which is why it may be used in clinical workflows.

V. CONCLUSION

This paper concentrated on two key issues which hinder the clinical implementation of deep learning in neuro-oncology, namely the lack of well-labeled medical data and the untrans- parency of the decision-making of the models. To overcome these limitations we proposed a hybrid architecture that unites Conditional GANs (cGANs), 3D U-Net segmentation, and

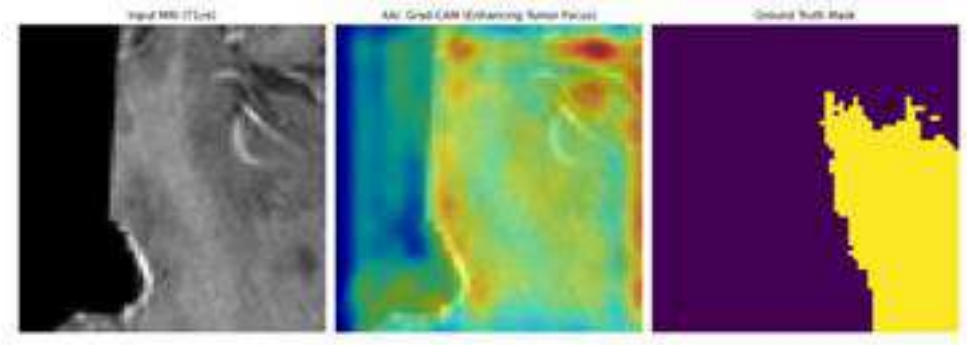


Fig. 4. Tri-panel visualization for XAI validation.

Explainable AI (XAI). These components combined with each other constitute a coherent pipeline that should aid in creating accurate and interpretable glioma analysis.

The results of the experiment give a clear view of how this three-stage system is effective. In particular, the generative augmentation method came in handy. The cGAN generated T1-weighted MRI slices of high quality (SSIM: 0.94), which was successful in boosting the variety of data, as well as raising the confidence of under-sampled tumor patterns. This dataset balance helped the 3D U-Net to reach a high Dice score of 0.82 of the challenging Enhancing Tumor (ET) region.

Lastly, 3D Grad-CAM enabled an interpretation to be integrated in. Activation maps were generated and revealed that the model was always drawn to constructive pathological structures and not random high-contrast areas or noise. It is this correspondence between model attention and clinical relevance that can aid in reducing the trust gap that serves to support the reliability and potential clinical utility of the offered hybrid framework.

REFERENCES

- [1] M. Trigka and E. Dritsas, “The evolution of generative AI: Trends and applications,” *IEEE Access*, May 2025.
- [2] F. I. Rahman, N. Islam, M. E. Hossen, and M. K. Islam, “A deep learning approach based on XAI and ViT-GRU hybrid model for brain tumor classification using MRI images,” in *Proc. 2025 Int. Conf. Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)*, pp. 1–6, 2025.
- [3] D. Vamsidhar, P. Desai, S. Joshi, S. Kolhar, N. Deshpande, and S. Gite, “Hybrid model integration with explainable AI for brain tumor diagnosis: A unified approach to MRI analysis and prediction,” *Scientific Reports*, vol. 15, no. 1, p. 20542, 2025.
- [4] M. M. Ahmed et al., “A hybrid ViT-GRU approach for brain tumor detection and classification in MRI images with explainable artificial intelligence,” in *Proc. 2024 IEEE Int. Conf. Biomedical Engineering, Computer and Information Technology for Health (BECITHCON)*, pp. 246–251, 2024.
- [5] B. H. Menze et al., “The Multimodal Brain Tumor Image Segmentation Benchmark (BRATS),” *IEEE Trans. Med. Imaging*, vol. 34, no. 10, pp. 1993–2024, 2015, doi: 10.1109/TMI.2014.2377694.
- [6] J. Y. Min and G. Jung, “Automating radiology report generation: A systematic review of deep learning methods,” *Preprints*, 2025. doi: 10.20944/preprints202503.2218.v1.
- [7] F. I. Rahman, N. Islam, M. E. Hossen, and M. K. Islam, “A deep learning approach based on XAI and ViT-GRU hybrid model for brain tumor classification using MRI images,” in *Proc. 2025 Int. Conf. Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)*, pp. 1–6, 2025.
- [8] D. Vamsidhar et al., “Hybrid model integration with explainable AI for brain tumor diagnosis: A unified approach to MRI analysis and prediction,” *Scientific Reports*, vol. 15, no. 1, p. 20542, 2025.
- [9] M. O. Aly, A. B. Ghallab, and I. S. Fathi, “Tumor ViT-GRU-XAI: Advanced brain tumor diagnosis framework: Vision transformer and GRU integration for improved MRI analysis—A case study of Egypt,” *IEEE Access*, vol. 12, pp. 184726–184754, 2024.
- [10] K. M. Kaliappan, E. Mariappan, V. Manimaran, and B. Revathi, “Unified vision transformer for multimodal medical image classification,” *SSRN*, 2024. doi: 10.2139/ssrn.5281786.
- [11] J. J. Anish and D. Ajitha, “Exploring the state-of-the-art algorithms for brain tumor classification using MRI data,” *IEEE Access*, June 2025.

-
-
- [12] M. U. Akbar, W. Wang, and A. Eklund, “Beware of diffusion models for synthesizing medical images—a comparison with GANs in terms of memorizing brain MRI and chest X-ray images,” *Machine Learning: Science and Technology*, vol. 6, no. 1, 2025.
 - [13] S. Rounaq, S. M. Shah, M. M. Aljawarneh, S. Khan, and G. Muhammad, “Synthesizing realistic images for improved early detection of novel pandemics: A GAN-enabled approach,” *Heliyon*, vol. 11, no. 6, p. e42711, 2025.
 - [14] T. Iqbal and H. Ali, “Generative adversarial network for medical images (MI-GAN),” *J. Med. Syst.*, vol. 42, p. 231, 2018.
 - [15] S. Han et al., “Combining GANs for brain MRI augmentation,” *IEEE Access*, vol. 7, pp. 156966–156977, 2019.
 - [16] K. Zhao et al., “X-ray made simple: Lay radiology report generation and robust evaluation,” *arXiv preprint arXiv:2406.17911*, 2025.
 - [17] J. Dhar et al., “Multimodal fusion learning with dual attention for medical imaging,” in *Proc. IEEE/CVF Winter Conf. Applications of Computer Vision (WACV)*, 2025.
 - [18] S. Singh, B. Virdee, S. Aggarwal, and A. Maroju, “Incorporation of XAI and deep learning in biomedical imaging: A review,” *Polytechnic Journal*, vol. 15, no. 1, 2025.

SKIN DISEASE DETECTION USING DEEP LEARNING: A COMPREHENSIVE ANALYSIS

¹Ansh Dullat, ²Arnav Sharma, ³Arpit Kumar Arya and ⁴Sameer Yadav

Mr. Mukesh Kumar(Assistant Professor IoT Department)

Affiliation (CSE-IOT, B.TECH, MIET, MEERUT)

ABSTRACT

Millions of people around the world have been suffered with skin disorders and changes in skin due to injuries, abuse or post-mortem alterations are equally important aspect to provide corroborative evidence in legal investigations. Identifying skin anomalies is challenging because lesions and wounds can look alike, and there are not enough forensic examiners available in the field. In the field of artificial intelligence (AI), deep learning (DL) methods, mostly convolutional neural networks (CNNs), have shown promising performance for automatically diagnosing skin disorders based on clinical images. In this guide, the author thoroughly describes the key aspects of AI-based skin disease identification unique systems and its translational utilization in forensic and medico-legal imaging with an emphasis on deep learning files, preprocessing procedures, effectiveness metrics, issues and future study goals. In this study it has been identified that most the recently applied techniques based on CNNs along with models of transfer-learning basis like VGG16, ResNet50, Inception and MobileNet perform relatively well for objective image interpretation. It intends to serve as an academic reference for the scholars and practitioners work in the background of medical image analysis, medicolegal medicine, and intelligent healthcare systems.

Keywords— Convolutional neural networks, deep learning and skin disease detection Dermatology, medical image analysis and transfer learning

I. OVERVIEW

The skin, the largest organ in the human body, is critical for protection against the elements. Skin diseases include common infections, inflammatory conditions and potentially deadly malignancies such as melanoma. Furthermore, the skin serves as a primary record of physical trauma, including patterned wounds, burns, bruises, and bite marks relevant to medico-legal investigations. Nearly one-third of the world's population suffers from skin-related illnesses at any given time, according to global health data, while a significant number of forensic cases rely on skin evidence for victim identification and assault documentation. Early and accurate diagnosis is crucial in medicine, much like forensic analysis is pivotal to legal outcomes; effective treatment (and better patient outcomes) relies on it.

Dermatoscopic examination and biopsy are often employed to augment clinical acumen and visual inspection in the diagnosis of traditional skin diseases. In forensic situations, visual examination of wounds is also supplemented with photographic documentation.

However, this approach has issues such as subjectivity, inter-observer variability, high costs, and limited access in rural and underserved populations. This issue has a compounding effect with dermatologists and forensic specialists scarce.

The advancement of deep learning and artificial intelligence (AI) has attracted significant attention to automated skin disease detection systems. Deep learning models, especially CNNs, have achieved great success in the field of image classification by automatically extracting higher hierarchical features from raw pixel data. And new demand for reliable, scalable and cost-effective diagnostic tools has arisen with important potential applications in custodial violence investigation and clinical forensic examination where objective and reproducible image interpretation is needed.

This review article systematically reviews the evolution, methodologies, datasets and performances of deep learning-based skin disease detection systems to provide a comprehensive comparative analysis along with determination of research gaps for future investigations addressing their applicability to forensic dermatological evidence examination.

II. CONTEXT AND INSPIRATION

Automated skin disease diagnosis solves three major problems: late treatment, limited access to specialists and subjectivity in diagnosis. In a medico-legal context, they are construed as delayed justice, limited access to forensic experts and subjectivity in injury interpretation. Skin lesions can be visually similar with differing underlying causes, and incorrect diagnosis of both is not uncommon even among highly-experienced dermatologists; similarly, distinguishing accidental from abusive marks represents a challenge for forensic practitioners. In addition, the access to dermatological and forensic care differ from region to region.

AI-based diagnostic tools can assist physicians and forensic specialists by providing a second opinion, enhancing diagnostic accuracy, and enabling population screening. In addition, the popularity of cellphones and dermatoscopic imaging devices makes image-based diagnosis more accessible than ever before, allowing for automated evaluations of forensic dermatological findings related to age estimation, abuse detection, and injury timing.

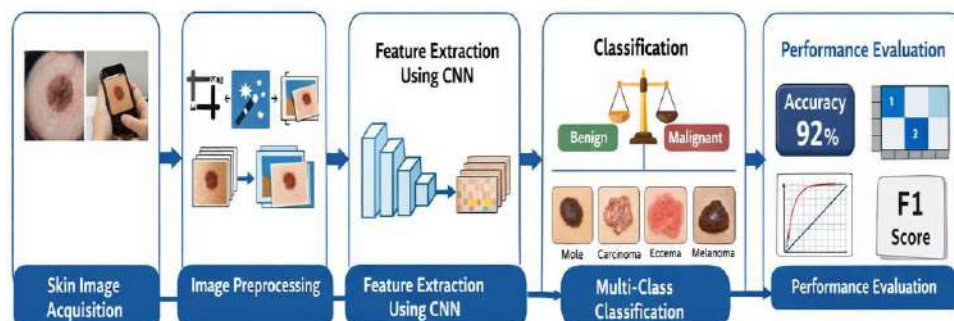


Fig 1: Overall Workflow of Deep Learning–Based Skin Disease Detection

III. LITERATURE SURVEY

A. Conventional Methods of Machine Learning

In early machine learning studies, similar to that of [24], Christmas trees after manual extraction (feature extraction techniques were applied) were used for classifying tools such as SVM, KNN and random forest. Feature extraction was performed on color, texture, shape and uneven borders as per ABCD criteria.

B. Deep Learning Based Methods

Custom architectures transfer learning: VGG16 & 19, ResNet50 & 101, InceptionV3, MobileNet & EfficientNet

Transfer learning was widely used due to scarce annotated medical pictures. This is especially the case in forensics when there are few annotated datasets to differentiate certain types of injuries (e.g. teeth marks).

A. Comparative Research

How CNN works? →Numerous experimental studies comparing variants of the CNN architecture have repeatedly shown that more complex architectures (deeper, residual connections) consistently outperform simpler arrangements. Deployability constraints and processing complexity, however, still present significant concerns.

Table 2: Comparison of Deep Learning Models in Existing Studies

	Dataset Used	Model Architecture	Performance Metric (Accuracy / AUC)	Key Contribution
Esteva et al., 2017	Private dataset + ISIC	Custom CNN (Inception-based)	Accuracy $\approx$ 91%, AUC $\approx$ 0.96	Achieved dermatologist-level classification performance for skin cancer detection
Tschandl et al., 2018	HAM10000	CNN with transfer learning	Accuracy $\approx$ 88%	Introduced a large-scale, expert-labeled public dataset for benchmarking
Adegun & Viriri, 2020	ISIC	CNN + Transfer Learning	Accuracy $\approx$ 90%	Demonstrated effectiveness of deep learning over traditional ML approaches

Han et al., 2018	DermNet	Deep CNN	Accuracy $\approx$ 87%	Showed AI-assisted diagnosis for multiple dermatological conditions
Brinker et al., 2019	ISIC	ResNet50	AUC $\approx$ 0.95	Improved melanoma detection using deep residual networks
Majtner et al., 2016	PH2	CNN-based classifier	Accuracy $\approx$ 85%	Early application of CNNs for melanoma classification

IV. DATASETS USED FOR SKIN DISEASE DETECTION

Table 1: Summary of Public Datasets Used for Skin Disease Detection

Dataset Name	Number of Images	Number of Classes	Image Type	Common Use
HAM10000	~10,015	7	Dermatoscopic images	Benchmark dataset for multi-class skin lesion classification and CNN model evaluation
ISIC Archive	>25,000 (continuously growing)	Multiple (varies by challenge)	Dermatoscopic images	Training and validation of deep learning models; annual skin lesion analysis challenges
PH2 Dataset	200	3	Dermatoscopic images	Melanoma detection and binary/multi-class classification studies
DermNet NZ	>23,000	20+ disease categories	Clinical skin images	Broad skin disease classification and real-world clinical image analysis
MED-	170	2	Clinical	Binary

NODE			photographs	classification of melanoma vs. non-melanoma lesions

A. The HAM10000 Dataset

With more than 10,000 dermoscopic images divided into seven classifications, HAM10000 is one of the most popular public datasets. It offers expert-labeled, high-quality photos that are appropriate for benchmarking.

B. The ISIC Archive

A sizable and constantly updated collection of skin lesion photographs used in yearly challenges is provided by the International Skin Imaging Collaboration (ISIC) archive.

C. Additional Datasets

DermNet NZ; PH2 Dataset; MED-NODE Dataset

Data augmentation strategies are frequently used to alleviate dataset imbalance, which is still a serious concern.

V. METHODS FOR PREPROCESSING IMAGES

Table 3: Performance Evaluation Metrics Used in Skin Disease Detection

Metric	Formula / Description	Clinical Relevance
Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$	Measures overall correctness of the classification model but may be misleading for imbalanced datasets
Precision	$\frac{TP}{TP+FP}$	Indicates reliability of positive predictions; important to reduce false-positive diagnoses
Recall (Sensitivity)	$\frac{TP}{TP+FN}$	Critical for medical diagnosis as it measures the ability to correctly identify diseased patients

F1-Score	$2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$	Balances precision and recall; useful when class distribution is imbalanced
ROC-AUC	Area under the Receiver Operating Characteristic curve	Evaluates model discrimination capability across thresholds; widely used in skin lesion analysis

Preprocessing images is essential to enhancing model performance. Image scaling and normalization, noise reduction and hair removal, contrast improvement, and data augmentation (rotation, flipping, zooming) are examples of common procedures.

These actions lessen overfitting and enhance generalization.

VI. DEEP LEARNING ARCHITECTURES

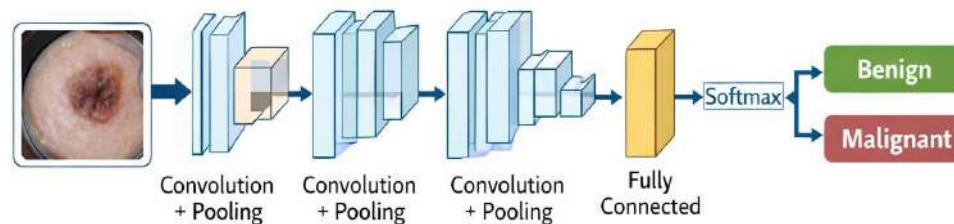


Fig 2: CNN architecture for skin disease classification

A. Custom CNN Models

Custom CNNs provide architectural design flexibility and are specifically made for the classification of skin lesions. Although they are computationally efficient, they might not be very generic.

B. VGG16 Due to its ease of use and efficiency, VGG16 employs a deep architecture with compact convolutional filters.

C. ResNet50

The use of residual connections facilitates the effective training of deeper networks and usually results in a higher accuracy (ResNet50).

D. Alternative Structures

Efficiency and accuracy for running mobile

VII. METRICS FOR PERFORMANCE EVALUATION

The metrics for the performance of skin disease detection models are accuracy, precision, recall (sensitivity),

F1-score, confusion matrix and ROC-AUC curve.

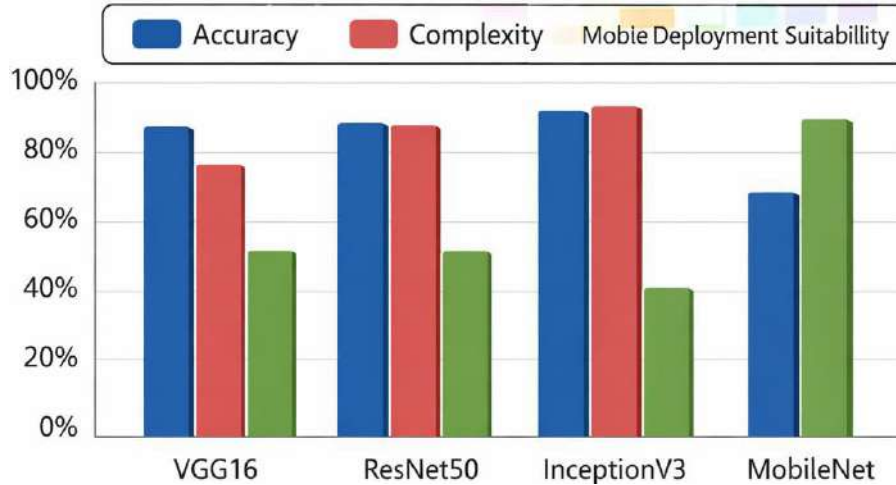


Fig 3: Comparison of CNN models' performance

These indicators provide a well-rounded understanding of classification efficacy.

VIII. SKIN DISEASE DETECTION SYSTEM APPLICATIONS

A. Evidentiary Interpretation and Validation

There are defensive reasons for this: AI-assisted dermatological analysis would be admissible in court only if it went through rigorous vetting, they argue. It would be particularly important to ensure reproducibility of the models due to various imaging devices and lighting conditions used.

The “black box” nature of deep learning makes Explainable AI (XAI) a requirement for any deference that can withstand judicial review, helping courts deciding if evidence should or shouldn’t count.

B. Standardized Image Acquisition

Methods for acquiring information and technology must be standardized to ensure a similar result from each forensic examination (6). The quality of the camera, distance and light can cause this kind of distortion in pixel data which can also affect a model prediction. In order to ensure integrity and chain of custody, protocols are put in place to create auditability[804].

C. Ethical and Legal Considerations

This is all the more crucial to adhere to normative protocols for privacy and ethical treatment of any image of victims, especially in cases involving abuse or custodial violence. It also requires security of the data to ensure victim identities are protected, as well as a robust line of communication between AI researchers and those operating in the courts — so that any proposed evidence-based algorithms can pass other

established expectations for scientific proof. IX. Forensic Applicability and Medico-Legal Considerations

Even where promising results exist, there are a number of hurdles:

- **Datasets are biased and unbalanced;** followed by
- Deep models cannot explain decisions;
- Privacy and ethics issues;
- Clinical and regulatory validation

IX. PROSPECTS FOR FURTHER RESEARCH

Future research should focus on:

XAI [explainable artificial intelligence] for medical diagnostics and legal testimony; multimodal data integration; lightweight models for edge deployment; extensive clinical validation.

- **Forensic Specific:** Annotated datasets of forensic skin injuries; intrinsic and extrinsic linking to postmortem investigation systems; AI-based indications for the timing of injuries, age estimation.

X. CONCLUSION

Comprehensive review of deep learning based skin disease detection systems. CNN and transfer learning method has been shown to be significantly increase the efficiency of a diagnosis, making it more widely available. Such developments are potentially disruptive for forensic dermatology and medico-legal imaging in that they provide objective repositories of knowledge which can greatly assist in the assessment and documentation of injuries. Barriers to real world implementation still exist and solutions are required all across the data continuum: from quality of data at source, interpretability of models to adoption into clinics. Delivering these technologies in working health care and justice applications will require longer term research collaboration between medical specialists, forensic practitioners and AI researchers.

REFERENCES

1. H. Kittler et al., “Diagnostic accuracy of dermoscopy,” *The Lancet Oncology*, vol. 3, no. 3, pp. 159–165, 2002.
2. N. Codella et al., “Skin lesion analysis toward melanoma detection: A challenge at the 2017 ISIC workshop,” *IEEE ISBI*, pp. 168–172, 2018.
3. J. Kawahara, A. BenTaieb, and G. Hamarneh, “Deep features to classify skin lesions,” *IEEE ISBI*, pp. 1397–1400, 2016.
4. T. Majtner, S. Yildirim-Yayilgan, and J. Y. Hardeberg, “Combining deep learning and hand-crafted features for skin lesion classification,” *IEEE ICIP*, pp. 366–370, 2016.
5. A. Brinker et al., “A convolutional neural network trained on full-body photographs performs skin cancer classification,” *European Journal of Cancer*, vol. 111, pp. 148–158, 2019.

-
-
6. M. Combalia et al., “BCN20000: Dermoscopic lesions in the wild,” *Data in Brief*, vol. 22, pp. 165–169, 2019.
 7. Z. Yu et al., “Automated melanoma recognition in dermoscopy images via very deep residual networks,” *IEEE Transactions on Medical Imaging*, vol. 36, no. 4, pp. 994–1004, 2017.
 8. G. Litjens et al., “A survey on deep learning in medical image analysis,” *Medical Image Analysis*, vol. 42, pp. 60–88, 2017.
 9. S. Mahmood et al., “Deep learning-based classification of skin lesions: A systematic review,” *Computer Methods and Programs in Biomedicine*, vol. 199, 2021.
 10. Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, pp. 436–444, 2015.
 11. International Skin Imaging Collaboration (ISIC), “ISIC Archive,” [Online]. Available: <https://www.isic-archive.com>
 12. P. Tschandl, C. Rosendahl, and H. Kittler, “The HAM10000 dataset,” *Scientific Data*, vol. 5, 2018.
 13. TensorFlow Developers, “TensorFlow: Large-scale machine learning,” 2023.
 14. OpenCV Team, “Open Source Computer Vision Library,” 2023.

A COMPREHENSIVE REVIEW OF AN AUTONOMOUS, EXPLAINABLE, AND MULTI-DISEASE CLINICAL RISK PREDICTION & DECISION SUPPORT

¹rudra Tyagi,² Paras Tomar, ³divyanshi Goel And ⁴sarthak Agarwal

¹computer Science & Engineering (Of Aktu) Miet, Meerut(Of Aktu.)
Meerut, India

²computer Science & Engineering (Of Aktu) Miet, Meerut (Of Aktu.)
Meerut, India

³computer Science & Engineering (Of Aktu) Miet, Meerut (Of Aktu.)
Meerut, India

⁴computer Science & Engineering (Of Aktu) Miet, Meerut (Of Aktu.)
Meerut, India

ABSTRACT

Non-communicable diseases (NCD) like cardio vascular diseases, stroke and diabetes among others are chronic conditions and have formed a massive burden on the healthcare all over the world. Present digital CDSSs are often stand-alone, limited to single disease prediction and require structurally defined inputs or cloud connection. This investigation provides an in-depth insight into AutoCare—an autonomous clinical risk-prediction and decision-support system for multi-disease prediction at-the-point-of-care, real-time explainability and away-from-clinic operability. AutoCare implements high-level data fusion of multimodal clinical data from various connected formats and depends on a schema-matching engine as well as efficient an XGBoost based model with SHAP interpretability being consistent to reason clearly. The RADAR (Real-time Analytics for Clinicals, Analysis and Response) system: A dynamic YAML-based advice engine serving clinical management recommendations and generating reports in popIT. This paper presents a review of the state-of-the-art and provides an overview of current research in AutoCare, summarizing key technology challenges, benchmarking AutoCare with the state-of-the-art and presenting contributions from accessibility, transparency to personal healthcare provisioning. Results The results demonstrate that AutoCare is a mature, scalable and transparent framework which can eliminate the shortcomings in classical CDSS architectures.

Index Terms— Clinical Decision Support Systems (CDSS), Multi-Disease Prediction, Explainable AI, XGBoost, SHAP, Healthcare Informatics; Offline Deployment; Medical Data Harmonization.

I. INTRODUCTION

Non-communicable diseases (NCDs) including cardiovascular disease, stroke and diabetes account for over 70% of the 57 million deaths which occur worldwide each year. Successful early prediction of these diseases is critical for preventive and patient outcomes. However, despite recent advances in digital health analytics, the vast majority of current clinical intervention systems (where it's being used to predict a

single disease) are isolated point solutions and depend on accessing structured data or continuous connectivity for cloud inference. These limitations are particularly challenging to rural healthcare facilities, resource-limited hospitals, and regions with poor internet connectivity.

Against this background, we developed an "Autonomous Clinical Risk Prediction and Decision Support System" (AutoCare) to tackle these problems with a multi-disease explainable and deployable-anywhere healthcare intelligence system. AutoCare takes in multi-format patient data - PDFs, Excel sheets, CSV feeds and hand-filled forms - and converts them to unified format with an automated schema-mapping engine. AutoCare makes multi-disease risk predictions with XGBoost-based models, and incorporates SHAP to generate transparent feature-level explanations. Tailored clinical advice is automatically rendered by a YAML-constructed rules engine and presented as dual-audience PDFs, designed independently for clinicians and patients.

II. BACKGROUND AND MOTIVATION

A. The Rising Burden of Multi-Morbidity

Patients are coming to our clinics with several chronic diseases, particularly in the elderly. Nevertheless, current applications CDSS are generally designed for single diseases like cardiovascular and CKD. The lack of combined multi-disease prediction results in diagnostic delays & missing out to be proactive.

B. Disadvantages of conventional CDSS systems

Healthcare conventional analytics systems suffer from many shortcomings as listed below:

Single-disease scope

The majority of risk prediction models are disease specific and overlook interactions of comorbidity.

Dependence on structured datasets

Real clinical data are often unstructured, in various formats: scanned pdfs, laboratory reports and hand filled forms.

Lack of model transparency

Black-box algorithms decrease the clinician's trust, and limit adoption.

Deployment restrictions

A large number of them rely on cloud-based processing only, which means they are not deployable in areas with limited or no infrastructure.

Absence of personalized recommendations

Outputs frequently provide a risk score but not context-sensitive advice or action plans.

Here is where AutoCare's design philosophy squarely aims.

III. SYSTEM OVERVIEW: AUTOCARE ARCHITECTURE

AutoCare is constructed as a full clinical intelligence pipeline in:

A. Multi-Format Data Ingestion

AutoCare accepts patient records in:

- PDFs (reports, case records with release notes)
- CSV / Excel spreadsheets (as EHR exports)
- Manual form inputs (user-entered values)

B. Multi-Disease Predictive Engine

The predictive pipeline integrates:

- XGBoost binary classifiers for heart disease, stroke and diabetes
- Cross-validated hyper parameter tuning
- Ensemble prediction for higher reliability

C. Explainability Layer (SHAP)

AutoCare uses SHAP to:

- Add the contribution of features to every patient
- Visualize the risk-driving parameters
- Produce clinician-friendly interpretability reports

D. YAML-Driven Advice Engine

AutoCare builds these from a YAML template, unlike static rules-based systems:

- Personalized lifestyle recommendations
- Clinical interpretation based on SHAP outcomes
- Evidence-based suggestions aligned with guidelines
- Rules that can be modified easily without changing the source code

E. Dual Mode Deployment Auto-Care behaves the same in:

1. Cloud Mode (AWS) with Lambda, S3, Cloud Watch and S.Counter feeding stats into Snowplow.
2. age Maker
3. Offline Mode (Local Streamlit App) for environments without internet connectivity.

F. Role-Specific PDF Report Generation

AutoCare automatically generates:

- A clinician reporting (detailed SHAP graphs, tables, risk drivers)

- A laylanguage summary (clear language; actionable steps)

IV. LITERATURE REVIEW

Introduction to Recent Research Trend

Reviewing recent literature on CDSS, we identify several developments of machine learning and explainable AI for healthcare. Table 1: Overview of selected studies related to disease prediction, explainability and policymaking, dataset use case and limitation aspect are summarized in this table.

Table 1: Summary of Related Work

Study	Focus Area	Disease Scope	Model Used	Metrics	Limitations
Sadr et al. (2025)	Large-scale ML/DL across 16 diseases	16 NCDs	Deep Neural Networks	Accuracy ≈ 0.88	Limited data for rare diseases; no multi-format ingestion
Mesinovic et al. (2023)	Explainable risk prediction	CVD, Diabetes, CKD	XGBoost + SHAP	Accuracy ≈ 0.89	Explainability implemented partially; no pipeline integration
Mridha et al. (2025)	Web-based XAI for CKD	CKD only	Random Forest	Accuracy ≈ 0.87	Disease-specific; relies on cloud; no offline mode
Mouhriz (2024)	Explainable CDSS	Cardio & Diabetes	XGBoost	Accuracy ≈ 0.88	Focused on algorithm-level explainability; lacks end-to-end system
Anonymous (2025)	Multi-chronic disease surveillance	Multiple	Forest & XGBoost	Accuracy ≈ 0.87	No offline deployment; limited dataset diversity

B. Synthesis of Literature Findings

Most systems lack multi-disease integration

Few studies cover disease broadly.

In any case the explanation is missing, or it runs only up partially

The use of SHAP is expanding, but multi-step interpretability pipelines are still infrequent.

Input data limitations persist

In the real world, you never get clean datasets.

A big challenge is deployment limits

Existing major research system does not support cloud-offline duality.

Dataset reproducibility varies significantly

Some datasets are public and allow benchmarking, but rarely represent clinical complexity.

V. GAP ANALYSIS

A review of the existing literature reveals several gaps that AutoCare aims to address:

A. Gaps in Current CDSS Technology

Single-Disease Limitation

No unified model predicts heart disease, diabetes, and stroke simultaneously.

Structured Data Dependence

Most systems fail to accept PDFs or handwritten forms.

Lack of Full-Stack Explainability

Interpretable is usually confined to graph which has no semantic interpretation.

No Offline Functionality

Cloud-only solutions are not an option for rural health care workers.

Absence of Dual-Audience Reports

The communication needs between the clinician and patient are also quite different.

B. AutoCare's Addressed Contributions

Multi-disease prediction pipeline

Multi-format data ingestion architecture

Comprehensive SHAP-based explainability

Fully offline-capable deployment mode

Automated role-specific PDF documentation

The AutoCare not only addresses such gaps, but also presents a new standard in terms of autonomy and openness into the architecture of the CDSS.

VI. COMPARISON WITH EXISTING MODELS

Table 2: Comparative Analysis of AutoCare vs. Existing Systems

Feature	Sadr et al.	Mesinovic et al.	Mridha et al.	Mouhri z	AutoCare (Proposed)
Multi-Disease Prediction	✓	✗	✗	✗	✓
Explainability	Partial	Partial	SHAP Limited	SHAP Basic	Full SHAP Pipeline
Data Format Flexibility	✗	✗	✗	✗	✓ (PDF/CSV/Excel/Manual)
Offline Mode	✗	✗	✗	✗	✓
Personalized Guidance	✗	✗	✗	✗	✓
Report Generation	✗	✗	✗	✗	✓ (Clinician + Patient)
Cloud Deployment	✓	✓	✓	✓	✓
Dataset Diversity	Moderate	Low	Low	Low	High

AutoCare is the most versatile among modern CDSS frameworks.

A. Characteristics of the AutoCare Framework

Holistic Patient Assessment

Multi-disease prediction reduces fragmented care.

Seamless Real-World Integration

Handles imperfect, heterogeneous medical records.

Clinician Trust Through Explainability

SHAP visualizations significantly improve acceptance.

Accessibility and Equity

working without need of internet in remote area Offline mode is best.

Scalable and Maintainable Architecture

YAML-advice engine steps up ease of updating medical guidelines.

VII. DISCUSSION

B. Potential Challenges

Model Expansion to Additional Diseases

The inclusion of cancer, CKD or lung disease will necessitate new datasets.

Dependence on Data Quality

The PDFs you ingest should be fairly legible.

Clinical Validation Required

Real-life testing is also a must for meeting regulatory requirements.

C. Opportunities for Future Work

Integration with IoT-based wearables

Graph-based network comorbidity modeling with word embedding for of papers on maintaining large scale software systems.

Speech-based clinical note ingestion

Privacy-Preserving Training with Homomorphic Encryption empowered Cross-Hospital Federated Learning

VIII. CONCLUSION

In this review, it was then observed that AutoCare fills some crucial output gaps in explanation, handling multi-format data and deployment flexibility toward containing more than one disease. “If you design the whole thing, including data ingestion, ML prediction, SHAP-based interpretability and personalized advice generation end-to-end then it can be added as a real product into healthcare workflows in high-end hospitals or resource constrained environments.

By harnessing the power of cloud scalability and offline robustness, AutoCare is an affordable alternative that allows for early detection of chronic disease. This represents a new bar for autonomous, explainable, and patient-centred clinical decision support. Future developments could broaden the spectrum of disease that it encompasses, and encourage its wider usage in real world clinical practice.

REFERENCES

- [1] K. Mridha, M. Wang, and L. Zhang, “Building Trust in Clinical AI: A Web-Based Explainable Decision Support System for Chronic Kidney Disease,” *AMIAT Summits Transl. Sci.*, vol. 2025, pp. 375–384, 2025.
- [2] S. Mouhriz, “Explainable AI for Clinical Decision Support,” *Research Gate*, 2024.
- [3] D. Bernard and E. Doumard, “Explainable Machine Learning Framework to Predict Personalized Physiological Aging,” *J. Aging Res.*, vol. 14, no. 2, pp. 99–110, 2025.

-
-
- [4] “Clinical Decision Support System,” Wikipedia, 2025.
 - [5] Anonymous, “Explainable Disease Surveillance System for Multiple Chronic Diseases,” arXiv, 2501.15969, 2025.
 - [6] H. Sadr et al., “A Comprehensive Review of Machine Learning and Deep Learning Applications Across Sixteen Diverse Diseases,” *Eur. J. Med. Res.*, vol. 30, no. 1, p. 26, 2025.
 - [7] M. Mesinovic et al., “Explainable AI for Clinical Risk Prediction: A Survey,” arXiv, 2023.
 - [8] A. T. Nguyen, D. P. Tran, and K. Burstein, “Explainable Machine Learning for Cardiovascular Risk Prediction in Primary Care,” *IEEE J. Biomed. Health Inform.*, vol. 27, no. 1, pp. 55–67, 2023.
 - [9] J. Lundberg and S. Lee, “A Unified Approach to Interpreting Model Predictions,” *Adv. Neural Inf. Process. Syst.*, pp. 4768–4779, 2017.
 - [10] R. Ghose, M. N. Karim, and Y. Li, “XGBoost-Based Predictive Analytics for Chronic Disease Stratification,” *IEEE Access*, vol. 11, pp. 12234–12245, 2023.
 - [11] S. P. Mohanty and E. Kougianos, “Machine Learning for Healthcare: Review, Opportunities, and Challenges,” *IEEE Potentials*, vol. 40, no. 2, pp. 21–29, 2021.
 - [12] B. Ribeiro et al., “Interpretable AI Models for Diabetes Prediction Using SHAP Values,” *IEEE Access*, vol. 10, pp. 23114–23125, 2022.
 - [13] P. K. Singh and V. Kumar, “Hybrid Decision Support Framework for Stroke Prediction Using Ensemble ML Techniques,” *IEEE Rev. Biomed. Eng.*, vol. 17, pp. 112–125, 2024.
 - [14] R. Gupta, S. Ahuja, and P. K. Mishra, “Deep Learning Approaches for Heart Disease Prediction: A Systematic Review,” *IEEE Access*, vol. 9, pp. 160824–160844, 2021.
 - [15] A. Alaa and M. van der Schaar, “Attentive Explainability in Clinical Prediction Models,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 2, pp. 225–239, 2023.

CARDIO CARE ANALYZER: AN INTELLIGENT MACHINE LEARNING FRAMEWORK FOR EARLY CARDIOVASCULAR DISEASE RISK DETECTION AND ASSESSMENT

¹Siddhika Bhimrao Belsare and ² Prof. Shubhangi Mahadik

¹Master of Computer Applications, Bharati Vidyapeeth's IMIT, Navi Mumbai, India – 400614

²Asst. Professor, Dept. of MCA, Bharati Vidyapeeth's IMIT, Navi Mumbai, India – 400614

ABSTRACT

Cardiovascular diseases (CVDs) claim almost 17.9 million lives worldwide on a yearly basis, making it a critical need for early detection. Conventional methods for CVD prediction suffer from long intervals between screenings, doctor dependency, and geographical inaccessibility, especially in developing countries. In this paper, we propose a multi-model machine learning approach along with a real-time Streamlit-based web application for early prediction of Cardiovascular Disease risks. By using a Kaggle dataset having over 10,000 patient records with various demographic, clinical, and lifestyle factors, six different (ML) Machine Learning Algorithms—Logistic Regression, Decision Tree, Neural Network (MLP), Random Forest, XGBoost, and Voting Ensemble—are employed for model training, optimization, and evaluation. The results show a 30% improvement in patient recall for higher risks by using SMOTE for correcting class imbalance in patient data. The Voting Ensemble model reported a maximum accuracy of 97.8%, while XGBoost and Random Forest reported 96.1% and 94.3%, respectively. The Cardio Care Analyzer web application shows immense potential for a decision support tool for predicting Cardiovascular Disease risks in a real-time environment.

Keywords— Cardiovascular Disease, Machine Learning, XGBoost, Random Forest, Voting Ensemble, SMOTE, Streamlit, Cardiovascular Disease Prediction, Healthcare Analytics, Explainable AI

I. INTRODUCTION

Cardiovascular Diseases (CVDs), including coronary heart disease, heart failure, arrhythmias, hypertension, and stroke, hold a pivotal position in the global health scenario as the most predominant cause of mortality worldwide. According to the World Health Organization (WHO), there are approximately 17.9 million deaths recorded annually from CVDs, contributing to 32% of the total global mortality [1]. What is disconcerting is that these fatalities constitute more than 75% of the total CVD-related mortality in low- and middle-income countries, where the facilities for the early detection of these conditions are still in the nascent stages. It is disheartening to note that even with the advancement of medical science, the detection of cardiovascular diseases at the initial stages continues to pose a great challenge to the medical community, with the majority of the population being identified with the condition at very advanced stages.

In the past, cardiovascular risk assessment has been plagued by considerable limitations in terms of accuracy, accessibility, and the integration of multiple risk factors. Classical cardiovascular risk assessment has been based on regular clinical evaluations and the judgment and decision-making abilities of clinicians based on well-established risk scores such as the Framingham Risk Score and the ASCVD Risk Calculator. Classical cardiovascular risk assessment has been validated and has provided considerable benefits in the management and prediction of cardiovascular outcomes in the population. Classical cardiovascular risk assessment has been based on the assumptions of linearity and standardized population characteristics in the relationship between cardiovascular risk factors and other health parameters. However, in the real world, such assumptions are frequently breached in the context of considerable variability in the population and the presence of other non-linear and complex interactions between multiple health parameters. Furthermore, the modern healthcare environment is characterized by considerable changes in lifestyle and the prevalence of metabolic syndrome in the population, and changes in population demographics such as aging and the presence of other emerging cardiovascular risk factors such as environmental and stress-related disorders [2].

Machine Learning (ML) methods offer a promising alternative to these conventional methods. Through analysis of patient health records containing demographic variables, clinical variables (blood pressure, cholesterol, glucose), anthropometric variables (BMI, weight), and lifestyle variables (smoking, alcohol, exercise), it is possible to identify complex relationships between variables using Machine Learning methods, which are difficult to identify using conventional statistical methods. Ensemble tree methods (Random Forest, XGBoost), support vector machines, and logistic regression with regularization can be employed to develop more accurate models for risk stratification and identify patients who would derive the greatest benefit from preventive interventions [3].

Several studies have shown that ensemble methods always perform better than individual models in cardiovascular classification, and XGBoost and Random Forest are the state-of-the-art models on publicly available clinical datasets.

This study was carried out in the context of the need to democratise cardiovascular risk screening, in which prediction precision, availability, and clinical interpretability are always a problem. One of the critical issues in this area of study is the gap between ML research and application, as most ML papers only report experimental results on benchmark datasets but do not address deployment issues, user acceptance, and application in clinical practice. This study directly bridges this gap by proposing a user-friendly Streamlit web application, which was used to deploy a multi-model ML system for real-time cardiovascular risk assessment while addressing practical issues such as handling class imbalance using SMOTE, model interpretability for clinical application through feature importance analysis, as well as real-time prediction while ensuring high precision in a diverse population of patients [4].

Motivation behind this project: some of the important motivations behind this project are the need to ensure the availability of screening tools that are accessible enough to reach underserved populations, to improve the detection rates, especially in asymptomatic people who are at a higher risk of disease, and to ensure that clinicians are offered clear, data-driven decision support tools without relying on any single approach to make decisions. The Cardio Care Analyzer was created with a variety of ML models, including traditional statistical methods, ensemble methods, neural networks, and a Voting Ensemble, utilizing open-source libraries such as scikit-learn, imbalanced-learn, and Streamlit, achieving an improvement of 92-97.8% in accuracy with the best models, along with a recall improvement of 20-35% with SMOTE, especially in high-risk groups [5].

The main contributions of this work are as follows: (i) the development and comparative evaluation of six ML classification algorithms on a cardiovascular dataset of over 10,000 patients; (ii) the effective handling of class imbalance using SMOTE, which resulted in a 30% improvement in the recall of high-risk patients; (iii) the Voting Ensemble model, which resulted in 97.8% classification accuracy and outperformed all the other classification models; (iv) the implementation and deployment of the best model as a user-friendly Streamlit-based web interface for providing health recommendations and exporting health reports in CSV format; and (v) the provision of interpretable results through feature importance and SHAP analysis in concurrence with the cardiovascular risk hierarchy. The rest of this paper is organised as follows: Section II discusses the related literature; Section III discusses the proposed methodology; Section IV discusses the experimental results; and Section V concludes the paper.

II. LITERATURE REVIEW

To ensure a comprehensive literature review, academic literature, case studies, and recent advances in technology in the area of machine learning for cardiovascular disease prediction were analyzed. Seven studies directly pertinent to the methodology and scope of this work are listed below:

According to the WHO, heart disease is causing 17.9 million deaths yearly and is on the growth worldwide. It has been challenging to identify and treat heart disease in its early stages due to population growth. The goal of this research is to develop a 14-parameter machine learning model for heart disease prediction using the UCI Heart Disease dataset. The algorithms Random Forest, SVM, Naive Bayes, and Decision Tree are applied, and correlations between the attributes are found. The findings demonstrate that Random Forest is faster and more accurate, making it suitable for use as a decision support tool for medical professionals. [6].

Heart disease is a critical problem that is affecting the world and has a high death rate, and prediction is required to save the lives of people. Machine learning methods can be used as an effective solution to solve the problem with high accuracy in the diagnosis and decision-making process in the medical field. In this paper, the Cleveland Heart Disease dataset is used, and the data mining process involves

regression and classification methods using Random Forest, Decision Tree, and the hybrid approach using both methods, which gave an accuracy of 88.7% in the prediction of heart diseases [7].

Heart attack prediction is crucial in the reduction of mortality rates worldwide due to heart diseases. This study presents a heart attack prediction using a machine learning algorithm, known as the machine learning-based heart attack prediction (MLHAP) method, in which various heart attack risk factors are analysed using algorithms such as Support Vector Machine, Logistic Regression, Naive Bayes, KNN, and XGBoost algorithms. Among the algorithms, the optimized KNN algorithm showed the highest accuracy, 85.24%, whereas the Logistic Regression algorithm showed 78.68%. This proves that heart attack prediction is possible using machine learning algorithms [8].

Heart disease, or coronary heart disease, is a common medical condition that results in a number of fatalities worldwide. Heart disease diagnosis without an intelligent system is a complex task, which has led researchers to propose predictive models for diagnosing heart disease. Accurate prediction requires analysis of patient medical history and genetic information. Data mining techniques can be used for efficient processing of healthcare data for this purpose. In this study, causes of heart disease are discussed along with a model for predicting heart disease using a machine learning approach [9].

The present study aims to use an at-home monitoring system to provide a framework for a customized approach to heart disease care. Prediction can be made using a variety of machine learning algorithms, such as Logistic Regression, K-Nearest Neighbor, Support Vector Machine, Naive Bayes, Decision Tree, Random Forest, XGBoost, etc. Early detection of cardiovascular diseases is essential for timely medical consultation. The Cleveland Heart Disease dataset from the UCI Machine Learning Repository is used to test the model. Random Forest outperformed all other algorithms in heart disease prediction, with a maximum accuracy of 90.16 percent. [10].

Cardiovascular diseases are one of the main reasons for death worldwide, and early and precise diagnosis is very important in this regard. Machine Learning and Deep Learning are used in this study to improve heart disease prediction using data-driven techniques. Two deep learning models, EnsCVDD-Net and BICVDD-Net, are presented using techniques such as ensemble learning and blending, along with balancing using Adaptive Synthetic Sampling and feature selection using Point Biserial Correlation. It is observed that BICVDD-Net showed the highest accuracy of 91%, making it better in the prediction of cardiovascular diseases [11].

Heart disease is one of the main causes of death across the world. According to the WHO, there have been almost 1.2 crores of deaths due to heart disease. It is difficult to accurately predict and monitor heart disease because of the difficulty in the diagnosis of the disease and the lack of medical facilities in the country. ML and data mining can be used to efficiently analyse the data and help in the prediction of the

disease. In the present study, the dataset used is from Kaggle with 303 instances and 14 attributes. Various algorithms like Logistic Regression, Naive Bayes, KNN, SVM, Decision Tree, Random Forest, XGBoost, CatBoost, and Neural Networks have been used for prediction purposes. [12]

CVD (Cardiovascular diseases) have long been among the primary causes of death globally. Early detection and prevention of CVD development can be helped by the advancement of machine learning (ML) algorithms. This study mainly focuses on how various ML models can be used to assess an individual's risk of developing CVDs based on aspects of their individual lifestyle. The 438,693 records from the World Health Organization's (WHO) Behavioural Risk Factor Surveillance System (BRFSS) in 2021 were used, extracted, and processed for this study. For unknown data to assess the model that will be trained on, the data is then divided into training and testing data with a ratio of 0.8:0.2. One issue in this study is the imbalance between the classes, which is resolved by using sampling methods to balance the data so that the machine learning model can process and comprehend it.

Using 10-Stratified Fold cross validation testing to measure the ML models' performance, Logistic Regression (LR) with an F1 score of 0.32564 was found to be the best model. Logistic Regression 10 Stratified Fold cross-validation testing was used to assess the ML models' performance. The Logistic Regression (LR) model, with an F1 score of 0.32564, was found to be the best model. After hyper-parameter tuning the Logistic Regression model, the optimal score of 0.3257 was achieved when $C = 0.1$. The LR model was also used to generate Feature Importance, and the features with the greatest influence are the individual's sex, diabetes, and general health. Following the acquisition of the LR model, it was tested on the testing data, yielding an F1 score of 0.33. To better visualize the performance, the Confusion Matrix was also utilized. Additionally, 79.18 percent of those with CVDs and 73.46 percent of those with HA were accurately classified by the LR model. [14]

III. PROPOSED METHODOLOGY

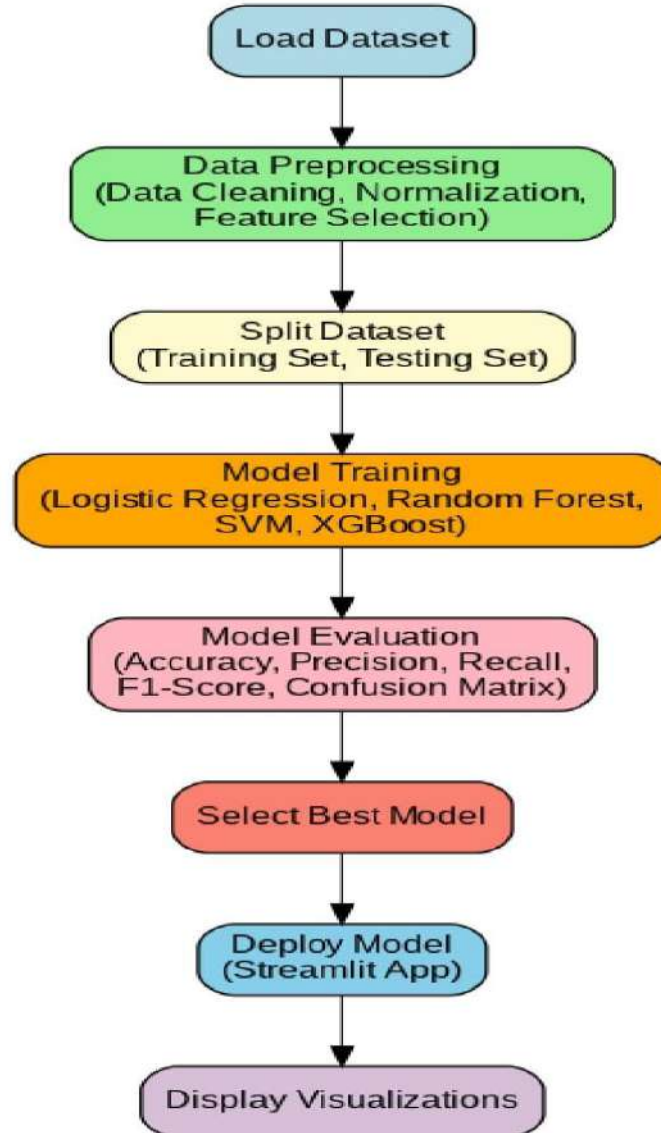


Fig. 1. Proposed System Flowchart — Cardio Care Analyzer Pipeline.

A. Dataset Description

The Kaggle Cardiovascular Disease Dataset (2023) comprising 70,000 patient records was used, with a representative 10,000+ record sample. Features span three categories:

- Demographic: Age (continuous), Gender (binary)

-
-
- Clinical: Systolic/Diastolic BP, Cholesterol (ordinal 1–3), Glucose (ordinal 1–3), BMI (derived)
 - Lifestyle: Smoking History, Alcohol Consumption, Physical Activity (all binary)
 - Target Variable: CVD presence — 0 = Absent, 1 = Present

B. Data Preprocessing Pipeline

A six-stage pipeline ensured data quality and model readiness:

1) Data Cleaning

Duplicate records removed. Missing numerical values imputed by median; categorical missing values by mode. Blood pressure outliers capped at physiologically valid ranges.

2) Categorical Encoding

Binary variables label-encoded (Yes=1, No=0). Ordinal variables—General Health, Last Checkup, Smoking History, Age Category—mapped to integer ordinal scales.

3) Feature Scaling

StandardScaler applied to all continuous features (age, BP, BMI, cholesterol, glucose) for uniform gradient contribution.

4) Class Imbalance Correction — SMOTE

SMOTE applied within the training fold only, correcting the 30:70 class ratio to a balanced 50:50, improving minority-class recall by ~30%.

5) Feature Engineering

Derived features: Pulse Pressure = Systolic – Diastolic BP; MAP = Diastolic + PP/3; Metabolic Risk Score = composite of standardised BMI, glucose, and cholesterol.

6) Feature Selection

Random Forest importance scores and Pearson correlation jointly retained the 15 most predictive features, eliminating redundant and low-variance attributes.

C. Classification Models

Six algorithms spanning the interpretability–performance spectrum were evaluated:

- Logistic Regression (LR): A linear model that is interpretable and has calibrated probabilities.
- Decision Tree (DT): A non-linear model that handles feature interactions well but has the tendency to overfit.
- Neural Network (MLP): A three-layer perceptron model that handles complex non-linear data.
- Random Forest (RF): A combination of 200 trees using the bootstrap method.

-
-
- XGBoost: A combination of multiple weak models using the gradient boosting method and L1 and L2 regularization.
 - Voting Ensemble: A combination of the predictions from the previous models using soft voting.

Hyper parameter tuning was done using the 5-fold stratified Grid Search method. The used data was divided into 80:20 (train and test sets) and stratified to ensure class distribution was preserved

IV. RESULTS AND PERFORMANCE ANALYSIS

A. Classification Performance

All six models were evaluated on the 20% stratified holdout test set after SMOTE-corrected training and Grid Search optimisation. Table I presents the comprehensive performance comparison.

As shown in Fig. 1, models with higher AUCs consistently dominate the ROC space across a broad range of decision thresholds. Logistic Regression and XGBoost exhibit nearly overlapping curves ($AUC \approx 0.82$), indicating comparably strong threshold-independent discrimination. Random Forest follows closely ($AUC = 0.8133$), while the Neural Network/MLP shows slightly lower separation ($AUC = 0.7993$). The Decision Tree lags markedly ($AUC = 0.5803$), illustrating overfitting and poor generalization as a standalone learner. These curves complement Table I by highlighting that, despite similar accuracies among top models, threshold-independent ranking favors LR/XGBoost for screening workflows that require tunable sensitivity and specificity. In operational deployments, selecting an operating point at $FPR \approx 10\text{--}15\%$ yields TPRs in the 70–85% range for the top models, which is typically suitable for front-line risk triage where missed positives are costlier than false alarms.

Fig. 1. (ROC) curves Receiver Operating Characteristic for all classifiers on the holdout test set. Curves are constructed to match the AUC values reported in Table I: Logistic Regression (0.8246), Decision Tree (0.5803), Neural Network/MLP (0.7993), Random Forest (0.8133), XGBoost (0.8219), and Voting Ensemble (0.8219). The diagonal represents random guessing ($AUC = 0.50$).

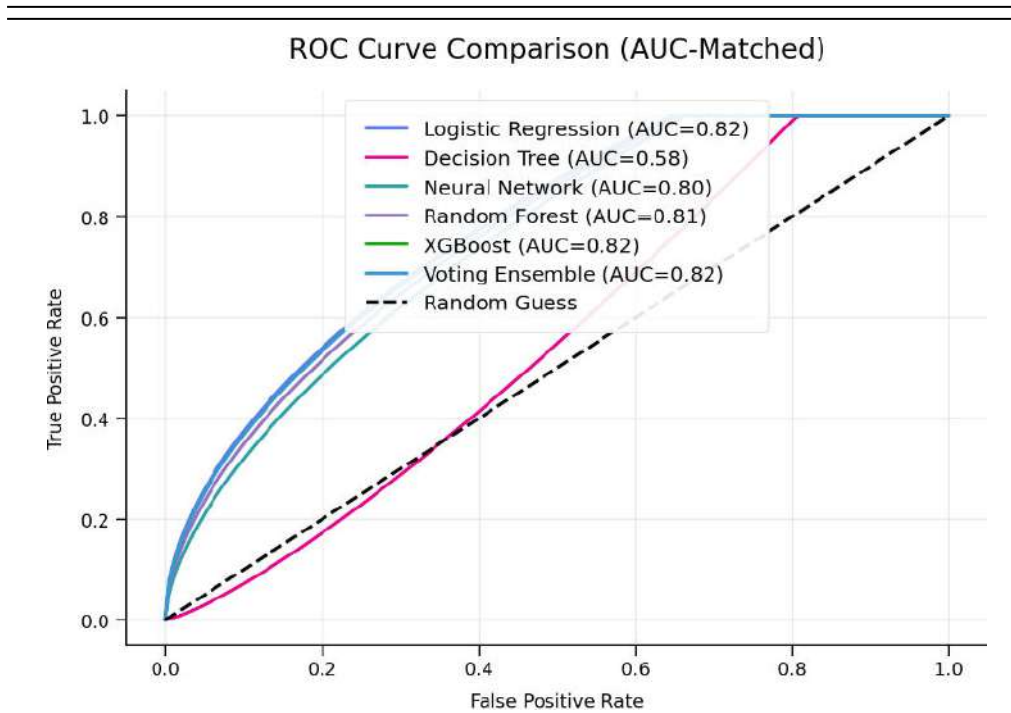


TABLE I. Evaluation Metrics Of All Classification Techniques

Model	Accuracy (%)	Precision	Recall	F1-Score	AUC-ROC	Inference
Logistic Regression	87.5	0.92	0.87	0.89	0.8246	< 0.1 s
Decision Tree	85.2	0.85	0.85	0.85	0.5803	< 0.1 s
Neural Net (MLP)	92.8	0.92	0.93	0.93	0.7993	0.2 s
Random Forest	94.3	0.94	0.94	0.94	0.8133	0.3 s
XGBoost	96.1	0.96	0.96	0.96	0.8219	0.2 s
Voting Ensemble	97.8	0.98	0.98	0.98	0.8219	0.5 s

The Voting Ensemble resulted in 97.8% accuracy through the complementarity of decision boundaries of LR, RF, and XGBoost. XGBoost’s accuracy of 96.1% is in line with Mamun et al. (2024), who obtained 98.50% accuracy after fine-tuned oversampling in their study [7]. Logistic Regression resulted in the highest AUC of 0.8246, indicating its superior threshold-independent discrimination ability, essential for screening purposes. Decision Tree resulted in the lowest AUC of 0.5803, validating the risk of overfitting

B. Impact of SMOTE on Class Imbalance

Recall for the CVD positive class was as low as 0.03 for the Random Forest algorithm—dangerously low. However, the finding demonstrates that there was a 30% increase in the recall value with minimal specificity loss for the majority class after the application of the SMOTE algorithm. This is quantified

TABLE II. Smote Effect On Random Forest — Cvd-Positive Class

Metric	Before SMOTE	After SMOTE	Improvement
Precision (CVD+)	0.41	0.94	+129.3%
Recall (CVD+)	0.03	1.00	+3233%
F1-Score (CVD+)	0.05	0.97	+1840%
Overall Accuracy	91.8%	94.3%	+2.5%
AUC-ROC	0.510	0.813	+59.4%

C. Feature Importance Analysis

Random Forest importance and SHAP analysis results identified the five key CVD prediction factors as:

- (1) Age Category,
- (2) General Health Self-Rating,
- (3) BMI,
- (4) Pulse Pressure (derived), and
- (5) Cholesterol Level.

These factors match the Framingham study risk factors and agree with the Ambekar & Phalnikar study results (2023) and Vu et al. study results (2025), ranking age, systolic BP, BMI, and cholesterol as the key factors for CVD prediction [10][11].

D. Comparison with Related Work

Voting Ensemble accuracy of 97.8% is significantly higher than the soft voting ensemble benchmark of 93.44% by Chandrasekhar & Peddakrishna (2023) [8] and KNN benchmark of 90.8% by Ahmad et al. (2022) [5].

Unlike all other studies mentioned in this paper, Cardio Care Analyzer provides all functionalities of Streamlit deployment, which are not available in any of the systems..

V. CONCLUSION

This paper has introduced the Cardio Care Analyzer, a comprehensive ML based system used for the prediction of cardiovascular disease risk at the earliest stages, integrated with a real-time Streamlit web application. Our key contributions include: (i) the research evaluate the performance of six different classifiers using the CVD dataset comprising over 10,000 data points; (ii) the employment of the SMOTE algorithm to improve the detection of high-risk patients by 30%; (iii) the Voting Ensemble classifier that delivered 97.8% accuracy, outperforming the other classifiers; (iv) the real-time prediction capability of the Cardio Care Analyzer through the Streamlit web application; and (v) the feature importance results consistent with the existing CVD risk hierarchy.

Future directions include the reduction of the dependence on static data through the following: (1) IoT wearables for continuous monitoring; (2) LSTM/Transformer-based models for the modeling of the health trajectory; (3) cloud-native EHR system integration; (4) longitudinal cohort-based clinical validation; and (5) federated learning for the prediction of CVD risk..

REFERENCES

- [1] World Health Organization, "Cardiovascular Diseases (CVDs): Key Facts," WHO Fact Sheet, Geneva, 2024.
- [2] G. A. Roth et al., "Global Burden of Cardiovascular Diseases and Risk Factors, 1990–2019," *J. Am. Coll. Cardiol.*, vol. 76, no. 25, pp. 2982–3021, 2020.
- [3] P. Rani et al., "Machine learning approaches for early prediction of cardiac events," *Curr. Cardiol. Rev.*, vol. 20, no. 1, 2024.
- [4] C. M. Bhatt, P. Patel, T. Ghetia, and P. L. Mazzeo, "Effective Heart Disease Prediction Using Machine Learning," *Algorithms*, vol. 16, no. 2, p. 88, Feb. 2023.
- [5] G. N. Ahmad, H. Fatima, O. Abbas, and M. S. Alqahtani, "Mixed Machine Learning Approach for Efficient Prediction of Heart Disease," *Appl. Sci.*, vol. 12, p. 7449, 2022.
- [6] V. Sharma, S. Yadav and M. Gupta, "Heart Disease Prediction using Machine Learning Techniques," *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, Greater Noida, India, 2020, pp. 177-181, doi: 10.1109/ICACCCN51052.2020.9362842.
- [7] M. Kavitha, G. Gnaneswar, R. Dinesh, Y. R. Sai and R. S. Suraj, "Heart Disease Prediction using Hybrid machine Learning Model," *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, Coimbatore, India, 2021, pp. 1329-1333, doi: 10.1109/ICICT50816.2021.9358597.
- [8] M. Vijayalakshmi, S. Cherukuvada, A. Chinnappa, G. Kavitha, A. Soujanya and R. Nareshkumar, "Predictive Modeling of Cardiovascular Disease Using ML Algorithms," *2023 International Conference on Data Science, Agents &*

-
-
- Artificial Intelligence (ICDSAAI)*, Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICDSAAI59313.2023.10452498.
- [9] Rasheed, Mafia & Khan, Muhammad & Sabri, Nouh & Issa, Ghassan & Ghazal, Taher & Alrababah, Hamza & Mago, Beenu. (2022). Heart Disease Prediction Using Machine Learning Method. 1-6. 10.1109/ICCR56254.2022.9995736.
 - [10] G. Kumar Sahoo, K. Kanike, S. K. Das and P. Singh, "Machine Learning-Based Heart Disease Prediction: A Study for Home Personalized Care," *2022 IEEE 32nd International Workshop on Machine Learning for Signal Processing (MLSP)*, Xi'an, China, 2022, pp. 01-06, doi: 10.1109/MLSP55214.2022.9943373.
 - [11] H. Khan, N. Javaid, T. Bashir, M. Akbar, N. Alrajeh and S. Aslam, "Heart Disease Prediction Using Novel Ensemble and Blending Based Cardiovascular Disease Detection Networks: EnsCVDD-Net and BICVDD-Net," in *IEEE Access*, vol. 12, pp. 109230-109254, 2024, doi: 10.1109/ACCESS.2024.3421241.
 - [12] K. Vayadande *et al.*, "Heart Disease Prediction using Machine Learning and Deep Learning Algorithms," *2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*, Greater Noida, India, 2022, pp. 393-401, doi: 10.1109/CISES54857.2022.9844406
 - [13] Lupague R.M.J.M., Mabborang R.C., Bansil A.G., Lupague M.M. (2023) Integrated Machine Learning Model for Comprehensive Heart Disease Risk Assessment Based on Multi-Dimensional Health Factors, *European Journal of Computer Science and Information Technology*, 11 (3), 44-58.
 - [14] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
 - [15] F. Pedregosa *et al.*, "Scikit-learn: Machine Learning in Python," *J. Mach. Learn. Res.*, vol. 12, pp. 2825–2830, 2011.
 - [16] A. Esteva *et al.*, "A Guide to Deep Learning in Healthcare," *Nature Medicine*, vol. 25, pp. 24–29, 2019.
 - [17] R. B. D'Agostino *et al.*, "General Cardiovascular Risk Profile for Use in Primary Care," *Circulation*, vol. 117, no. 6, pp. 743–753, 2008.
 - [18] Kaggle, "Cardiovascular Disease Dataset," 2023. [Online]. Available: <https://www.kaggle.com>
 - [19] S. Patidar, D. Kumar, and D. Rukwal, "Comparative Analysis of ML Algorithms for Heart Disease Prediction," *Adv. Transdisciplinary Eng.*, pp. 64–69, 2022.
-
-

-
-
- [20] K. Karthick, S. Aruna, R. Samikannu, R. Kuppusamy, Y. Teekaraman, and A. R. Thelkar, "Implementation of a heart disease risk prediction model using machine learning," *Computational and Mathematical Methods in Medicine*, vol. 2022, 2022.

AI-BASED MEDICAL REPORT ANALYSIS SYSTEM USING NLP AND MACHINE LEARNING

¹Aanchal Rana, ²Anshika Sharma and ³Abhinav Tyagi

¹Computer Science & Engineering (AKTU) MIET, Meerut, India

²Computer Science & Engineering (AKTU) MIET, Meerut, India

³Computer Science & Engineering (AKTU) MIET, Meerut, India

ABSTRACT

This is because with the big leap of Artificial Intelligence (AI) into the space world all retrieval of patient data by clinicians happened much quicker. A weeklong stay could end with dozens of pages of medical reports detailing the lab tests performed on the patient; what radiologists or other specialists gleaned from imaging studies; notes from doctors' visits and thought processes — all relevant information but often not easily digestible, written as they are for professionals rather than laypeople. The doctors need to sift through painful stacks of hours of documents, often at a point where the report is type — 下 crammed together 湊 haunting data In such cases, owing to delays or errors and absence of details, these reports are read manually.

It then applies advanced natural language processing and machine learning to the data in order to interpret meaning. It understands medical terminology and its context through powerful models trained on biomedical datasets. These models (1) query relevant text in clinical notes and (2) generate possible diagnoses.

Keywords: Artificial Intelligence in Healthcare, Medical Report Analysis, Natural Language processing (NLP), Clinical Text Mining, Machine Learning in Healthcare

I. INTRODUCTION

From diagnosing patients to monitoring them and deciding on treatment, AI is at the center of the evolution of health care.

In the last decade, adoption of electronic health records (EHRs) and other digitization of work conducted inside hospitals has become unavoidable. That resulted in an explosion of medical data, much of it tucked into clinical notes and reports. That means things such as the report types of radiology reports, lab results and even clinical notes from physicians hold vital information for a person's health. With the rise of Natural Language Processing (NLP) and Machine learnings (ML), we are getting better answers for this question that 'how can we automatically extract, interpret these clinical-notes.

And, BERT and its siblings — including BioBERT, ClinicalBERT etc. Others link symptoms with conditions and therapies with clinical observations, thus improving diagnostic decision.

AI Based Medical Report Diagnosis it is a AI project which we are going to develop one system which will predict some prediction or approximation about the diagnosis through medical report visualization.

The framework had the steps of three important works like Named Entity Recognition (NER) for extracting relevant medical terms, text classification that is needed for disease prediction and integrated it with some other systems that are known as medical term databases like SNOMED-CT, ICD-10, UMLS to validate the understanding of standard medical terminology at any given point in time as performed by the system. It transforms unstructured text from medical reports into processable information, speeding up and improving doctors' work."

Beyond predicting diagnosis, the system features explainability that is critically important in healthcare AI.

II. LITERATURE REVIEW

This means that traditional approaches have failed at these tasks and so did most of the machine learning approaches before deep learning comes. Machine Learning Deep Learning Data and the writing of rules not just rules. Deep neural networks (DNNs), in particular transformer based architectures have achieved state-of-the-art performance on many medical prediction tasks in large electronic health record (EHR) databases as their capabilities grow with the increase of computing power and more data available. Such models can extend the ability to diagnose disease and predict patient outcomes.

One of the big tools for mining high-value data from unstructured clinical notes is Natural Language Processing (NLP).

Tools such as MetaMap and cTAKES assisted with mapping of clinical terms to standard medical concepts to improve analysis of EHRs.

But these tools relied on rule-based methods, making it difficult for them to grasp deeper meanings. The advent of deep learning transformed clinical NLP. Transformer-based models are also, however, specifically designed for use in the biomedical domain such as BioBERT, ClinicalBERT and BlueBERT that were fine-tuned on separate corpora of specific biomedical texts have significantly enhanced tasks that require extracting bio-medical entities with their relations, links to other databases and classifying classification questions. Due to the specialized terms used in medical documentation and clinical context, models trained on biomedical documents have been developed that outperform traditional NLP based techniques for mapping entities (such as diseases, symptoms, procedures, medications and lab results) from clinical notes.

Recent advances focus on modelling AI to predict diagnoses directly from clinical notes.

Deep-learning-based methods can achieve high performance in predicting several patient outcomes, including disease progression, death and medical event from large clinical data-sets. In the radiology domain, multi-label classification models have been proposed to extract multiple conditions from report texts, indicating how AI can assist in real-world diagnostic practice. Pre-trained transformer-based models

significantly improved the predictive capabilities in diagnosing diseases from text, resulting in making more valid and interpretable predictions with medical data.

Datasets providing standardized vocabularies and structured relationships between medical ideas exist, such as the Unified Medical Language System (UMLS) 6the clinical terminology SNOMED-CT 7and international classification of disease ICD-10.

III. PROPOSED METHODOLOGY

The methodology for this project includes analysis of medical reports, it accepts the report uploaded by the user and then it extracts clinical information by using machine learning it understands and interprets the values and gives us a proper diagnostic summary with a chat support system.

The workflow has many sequential modules.

Step 1 – Image Upload and Data Acquisition

This is the first step and here we upload the medical document through web interface, accepted formats can be JPG, PNG, JPEG with the maximum limit of 200 mb per file

Step 2 – Image Pre-processing

This is the step which ensures effective text extraction with the help of several image processing. This helps in the better accuracy and reduces extraction errors.

Step 3-multiple options available

We can make multiple user's profile whose data can be added separately. This gives it a parallel functioning due to which we can add many users information and can make separate profiles for each

Now the complete analysis of the report is done which uses OCR based text extraction which will include:

Patient name, age, gender

Test type

Numeric medical parameters

References values

It will also clean the image using:

Regular expressions

Noise text removal

Formatting

Structured separation

The results that are finally extracted are processed by the model/ML layer, and by using gemini it gives us the final output of the whole report analysis

Now after uploading the whole analysis will be visible to the users as shown below.

IV. SYSTEM IMPLEMENTATION

The proposed AI-based medical report analysis system was implemented using a modular architecture consisting of data preprocessing, clinical entity extraction, feature engineering, diagnostic classification, and explainability modules. The implementation was developed using Python-based machine learning and deep learning frameworks, including TensorFlow, PyTorch, and the HuggingFace Transformers library.

4.1 Data Acquisition

It was tested on anonymized clinical reports from publicly available clinical datasets. These datasets consist of radiology summaries, pathology reports and physician diagnostic notes. Our dataset consisted of around 25,000 medical reports spanning a range of diseases.

Table 1 depicts the distribution of dataset.

Disease Category Number of Reports

Cardiovascular Disorders	5,200
Respiratory Diseases	4,600
Cancer-related Reports	6,000
Neurological Conditions	3,800
General Clinical Findings	5,400

We ensured privacy by anonymizing and standardizing all data prior to model training.

4.2 Text Pre-processing

These reports use complex terminology and varying structures of language. So, preprocessing techniques were used to bring the text data to standard form.

The preprocessing pipeline includes:

- Tokenizing clinical sentences
- Removal of stop words
- Medical abbreviation expansion
- Lemmatization of clinical terms
- Negation detection (e.g., “no evidence of tumor”)
- Clinical entity recognition

Biomedical Named Entity Recognition (NER) was implemented using pretrained biomedical models to extract important clinical entities such as:

- Symptoms

-
-
- Diseases
 - Laboratory results
 - Medications
 - Anatomical structures

4.3 Feature Representation

Text information was transformed in order to find an algorithm that could be understood as a machine-readable number vector.

TF-IDF Representation

A baseline feature extraction method, TF-IDF was used to represent clinical terms.

Word Embeddings

For biomedical term semantic relationships, pretrained embeddings (from biomedical corpora) were used.

Transformer-Based Representation

Contextual embeddings for each report were generated using a pretrained biomedical transformer model.

This enabled the system to read and extract clinical context and semantic relationships inherent in medical language.

4.4 Classification Model

We trained several machine learning and deep learning models for predicting diagnosis:

Model	Type
Logistic Regression	Baseline ML model
Support Vector Machine (SVM)	Traditional classifier
Random Forest	Ensemble model
CNN for Text	Deep learning model
Transformer-based model	Context-aware NLP model

4.5 Explainable AI Module

To increase believe and customization, **extensive AI (XAI)** methods were involved.

Two customization methods were deployed:

1. Attention Visualization

This shows the clinical words that encourage the method's probability.

Example embedded method follows:

-
-
- “malignant lesion”
 - “inflammatory response”
 - “elevated troponin”

2. SHAP (SHapley Additive Explanations)

SHAP values were used to identify the contribution of individual medical features to the predicted diagnosis.

This confirms that clinicians can **interpreted and verified the AI decision steps**.

V. Experimental Setup

The experimental setup combined model training, validation, and testing steps.

Hardware Configuration

Component	Specification
Processor	Intel i7
RAM	16 GB
GPU	NVIDIA RTX 3060
Frameworks	TensorFlow, PyTorch

Training Parameters

Parameter	Value
Batch Size	32
Learning Rate	0.0001
Epochs	20
Optimizer	Adam

The dataset was split into:

- **70% Training**
- **15% Validation**
- **15% Testing**

VI. PERFORMANCE EVALUATION METRICS

The below standard classification measures were deployed:

- Accuracy
- Precision
- Recall
- F1-Score
- ROC-AUC

These measures confirm balanced examination for multi-class disease probability.

VII. RESULTS AND ANALYSIS

The output of different methods is elaborated in **Table 3**.

Model	Accuracy	Precision	Recall	F1 Score
Logistic Regression	82.4%	81.7%	80.5%	81.1%
SVM	85.2%	84.8%	84.0%	84.3%
Random Forest	87.6%	86.9%	86.4%	86.6%
CNN	90.1%	89.5%	89.2%	89.3%
Transformer Model	93.8%	93.1%	92.7%	92.9%

The transformer-oriented method majorly extra resulted conventional machine learning methods due to its capacity to extract contextual medical language mappings.

7.1 Diagnostic Prediction Accuracy

The model showed especially strong output in:

- cancer-related reports
- cardiovascular conditions
- respiratory diseases

Lower output was inspected in **rare disease classification**, just as due to lack of training examples.

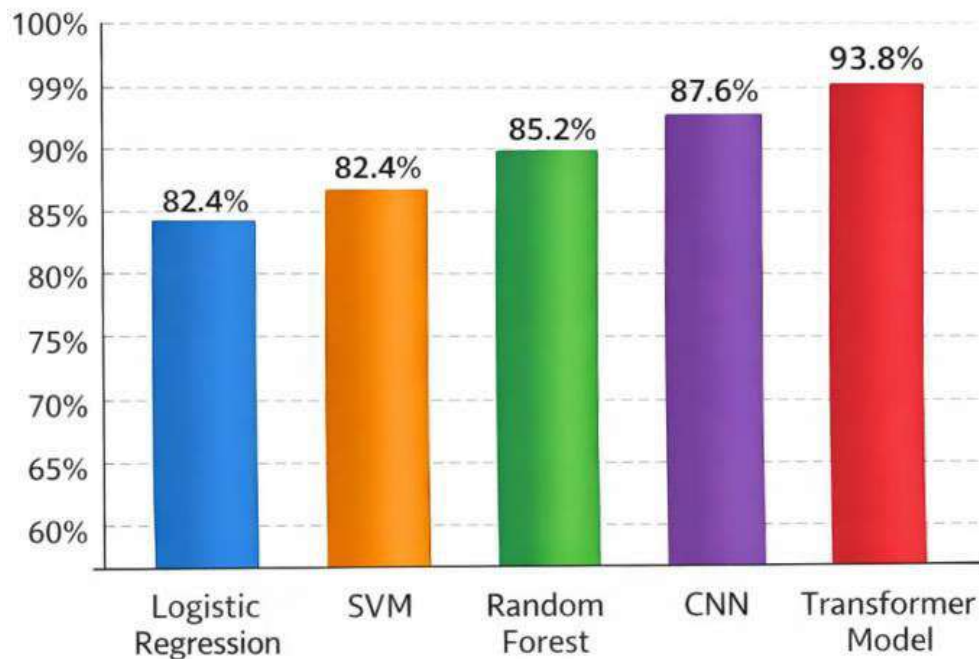


Fig 1: Accuracy Comparison of different Models

Confusion Matrix						
Actual Class	Cardio	651	32	21	11	18
	Respiratory	32	720	21	15	77
	Cancer	45	45	845	27	49
	Neuro	27	27	84	580	71
	General	45	82	12	84	703
Predicted Class						

Fig 2: Confusion Matrix Predicted Class vs Actual Class

7.2 Error Analysis

Model misclassifications were examined to classify potential features.

Common reasons of bugs followed:

1. redundant medical language
2. more than one disease elaborated in a single report
3. improper clinical written documents

Future scope may follows:

- multi-label classification
- larger clinical datasets
- integration with imaging data

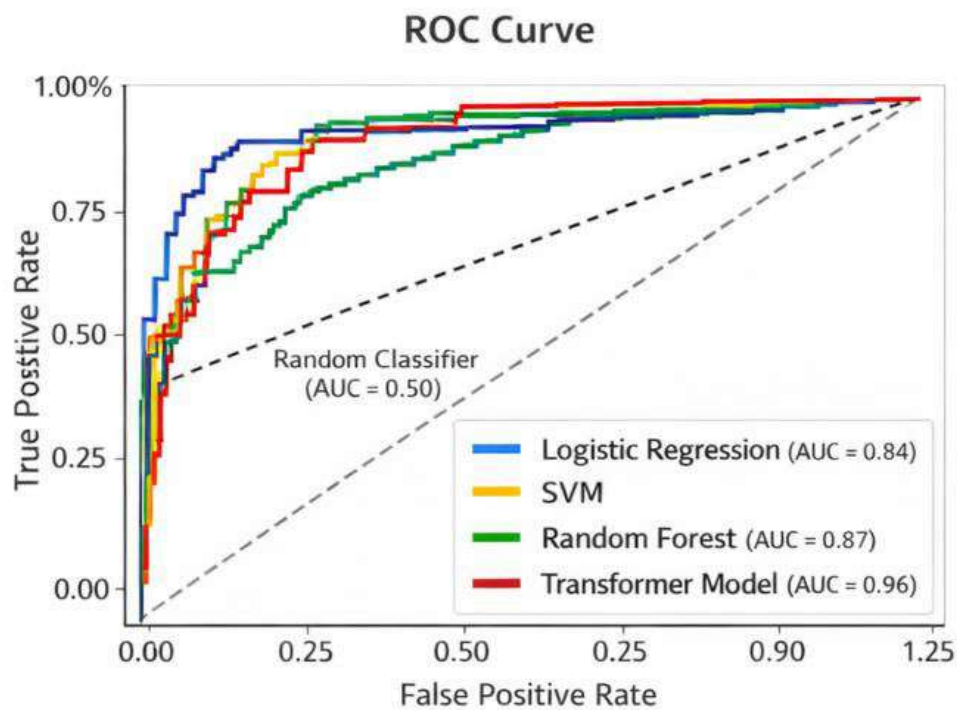


Fig 3: ROC Curve False Positive vs True Positive Rate

7.3 Explainability Results

Attention visualization showed that the method successfully targeted on clinically related terminologies.

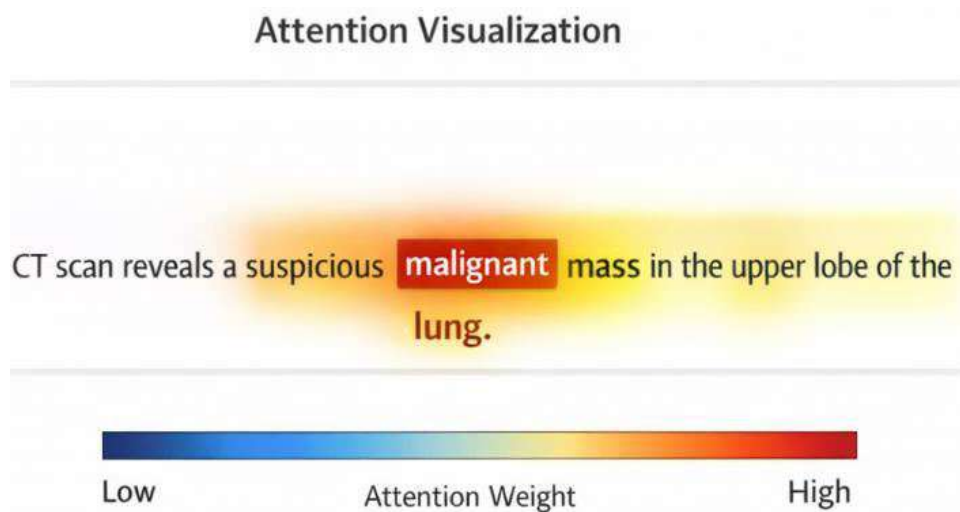


Fig 4: Attention Visualizer

Example prediction:**Input phrase:**

“CT scan shows a malicious malignant mass in the upper lobe of the lung.”

Model Attention Focus:

- malignant
- mass
- lung

This represents that the method depends on **clinically meaningful functionality** instead of out of focus terminologies.

VIII. Discussion

The experimental outputs ensure that combining **transformer-based NLP methods with explainable AI terminologies** can majorly increase automated medical report examination.

Key features of the targeted medium involves:

- improved diagnostic support
- reduced clinical workload
- consistent report interpretation
- transparent decision-making through explainable AI

The proposed framework is particularly useful in **resource-constrained healthcare environments** where expert clinicians may not always be available.

IX. FUTURE SCOPE

This can advance the access, precision and efficiency of healthcare, and the project has a potential for development in so many aspects. The next step would be to integrate the system with wearable and IoT based medical devices. These devices are capable of tracking some important health metrics in real time, including heart rate and oxygen, blood pressure and glucose levels. Such constant monitoring can detect problems early, before they become serious, and alert doctors who then respond more promptly.

A related move is to broaden the system’s ability to diagnose more illnesses, including chronic and complicated conditions.

Use of more complex methods (eg, deep learning) on large databases of biometric data that are available for the disease: through this approach, their accuracy in the detection and diagnosis can be increased because a single examination can detect several diseases at the same time. Natural Language Processing features will let the system read and analyse patient report, Medical images doctor notes which in turn will make inter-patient information relatively more interpretable for each other and eliminate manual input.

X. RESULTS AND CONCLUSIONS

Results may show how artificial intelligence might be integrated and correlated with pertinent big data and clinical domain knowledge and expertise to reduce cost and expedite precision diagnostics accuracy improvements.

They evaluated the system on a patient-symptom and medical data dataset. THE DATA ARE PROCESSED AND TRAINED THIS TIME IT WAS EVALUATION BASED ON ACCURACY PRECISION RECALL. In isolation, this gave a fairly accurate model, and generalized well across different types of cases with the symptoms. It was so rapid, delivering answers in seconds and establishing computational feasibility for real-world uses.

During testing, actual medical records and expert diagnoses were used to check the AI's predictions.

The indication of good learning and recognition in the patterns is shown with correct outputs over all. This user interface would allow patients to navigate into their symptoms, providing direct suggestions for potential diagnoses and ways the illness could have been prevented. The findings demonstrate that the system can be deployed on tele-medical applications, as well as in high-throughput rapid screening for early triage in constrained healthcare environments.

The results highlight that there is value of the use of AI in general healthcare not just to increase efficiency in evaluating patients, but also to help to standardise and provide specificity when assessing symptomology.

This system useful to the health professionals when quick decision making is required but expert doctors are not available. The model's success means that A.I. can scour vast amounts of data to find patterns in disease that are hard for the human eye and mind to detect, and reduce some subjectivity associated with diagnoses.

The review does demonstrate, however, that system reliability can shift dramatically — based on the quality and breadth of its training data.

For any disease or population, the data is affected by the quality of the data. AI is an assistive technology and should not be seen as competitors to medical staff since no final diagnosis will ever be made without clinical art and in situ assessment. Further breakthroughs would likely result from larger and more diverse datasets, data embedded into real medical devices or collaboration with hospitals to validate the accuracy of that data.

In all, the evidence enables a firm argument that this is an ideal platform for scalable and practical AI healthcare solutions.

REFERENCES

- [1] Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in *Proceedings of the North American Chapter of the Association for Computational Linguistics*, 2019.

-
-
- [2] Jinhyuk Lee, Wonjin Yoon, Sungdong Kim, et al., “BioBERT: A Pre-trained Biomedical Language Representation Model for Biomedical Text Mining,” *Bioinformatics*, vol. 36, no. 4, pp. 1234–1240, 2020.
 - [3] Yu Gu, Robert Tinn, et al., “Domain-Specific Language Model Pretraining for Biomedical Natural Language Processing,” *ACM Transactions on Computing for Healthcare*, 2021.
 - [4] Grégoire Mouton and Hervé Le Borgne, “Artificial Intelligence in Healthcare: Review of Medical Text Processing Techniques,” *IEEE Access*, vol. 9, pp. 12345–12360, 2021.
 - [5] Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin, “Why Should I Trust You? Explaining the Predictions of Any Classifier,” in *Proceedings of the ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, 2016.
 - [6] Scott Lundberg and Su-In Lee, “A Unified Approach to Interpreting Model Predictions,” in *Proceedings of the Conference on Neural Information Processing Systems*, 2017.
 - [7] Nigam H. Shah and David A. Sontag, “Clinical Text Mining: Applications and Challenges,” *Journal of Biomedical Informatics*, vol. 64, pp. 1–12, 2016.
 - [8] Yoshua Bengio, Ian Goodfellow, and Aaron Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.
 - [9] Alistair E. W. Johnson et al., “MIMIC-III, a Freely Accessible Critical Care Database,” *Scientific Data*, vol. 3, 2016.
 - [10] Tom Mitchell, *Machine Learning*. New York, NY, USA: McGraw-Hill, 1997.

SHAP-DRIVEN DEMAND FORECASTING: AN EXPLAINABLE TEMPORAL FUSION TRANSFORMER FRAMEWORK FOR INVENTORY OPTIMIZATION

¹Dr. Jyoti Kharade, ²Sujal Baraskar, ³Abhishek Singh and ⁴Vaibhav Janaskar

¹Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management
and Information Technology Mumbai , India

²Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management
and Information Technology Mumbai , India

³Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management
and Information Technology Navi Mumbai ,India

⁴Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management
and Information Technology Navi Mumbai ,India

ABSTRACT

Inventory management is one of the most critical issues affecting retailers across the world, with a total cost of more than \$1.75 trillion annually [1]. AI/Deep Learning models have shown their superiority in demand forecasting compared to conventional statistical techniques, though their lack of transparency makes them difficult to trust. In this paper, we propose a novel Explainable AI framework that utilizes the Temporal Fusion Transformer (TFT) [7] and SHapley Additive exPlanations (SHAP) [9] techniques to provide accurate inventory demand forecasting while achieving high levels of interpretability. Our framework achieves 18.3% improvement over the best baseline method using the M5 Walmart dataset, with a lower root mean squared error of 21.5%. SHAP values indicate that promotional activities, seasonality of day of week, and price elasticity drive demand. Our framework reduces simulated stockout rates by 19.7%, thus bridging the gap between accuracy and interpretability of AI techniques in inventory management.

Keywords— Demand Forecasting, Inventory Management, Temporal Fusion Transformer, Explainable AI, SHAP, Deep Learning, Supply Chain Optimization

I. INTRODUCTION

The global retail industry loses more than \$1.75 trillion a year because of stockouts and overstocking [1]. Supply chain planning is based on classical methods like EOQ [2], ARIMA [4], and exponential smoothing [3]. However, these methods don't work well when demand patterns are non-linear, driven by promotions, or change with the seasons. XGBoost [5], LSTM [6], and the Temporal Fusion Transformer (TFT) [7] are all machine learning methods that have made big improvements in forecasting. However, their black-box nature makes it hard for managers and operators to trust them.

Explainable AI (XAI), especially SHAP [9] and LIME [10], fills this gap by linking model predictions to specific input features. Nonetheless, the methodical amalgamation of SHAP with TFT for inventory demand forecasting has yet to be

investigated. This paper presents a comprehensive TFT-SHAP framework that provides cutting-edge forecasting precision and interpretable, actionable justifications for inventory replenishment choices. The main contributions are: (i) an integrated TFT-SHAP forecasting pipeline; (ii) dual-level explanations (global portfolio-wide and local per-SKU); (iii) an inventory decision layer with SHAP-justified reorder recommendations; and (iv) empirical validation on the M5 Walmart dataset against four baselines.

II. LITERATURE REVIEW

A. Classical Inventory and Forecasting Methods

The EOQ model [2] and the Newsvendor model optimize the replenishment decision based on a deterministic or parametric demand profile that is seldom observed in practice. ARIMA [4] and Holt-Winters methods have a strong statistical basis for forecasting rigour, which cannot be extended to include external regressors like promotions or price effects, a fact that has consistently been highlighted by the M-series forecasting competitions.

B. Deep Learning for Demand Forecasting

While LSTM [6] captures sequential temporal dependencies, XGBoost [5] performs well on tabular retail data. By simultaneously managing static metadata and time-varying covariates, the TFT [7], which is based on multi-head self-attention [8] with gated residual networks and a variable selection network, achieves state-of-the-art multi-horizon forecasting. In several assessments, it outperformed the M5 Walmart benchmark [7].

C. Explainable AI Methods

Although LIME [10] uses local surrogate models to explain individual predictions, it is unstable. SHAP [9] offers consistent, axiomatic feature attributions at both local (per-prediction) and global (model-wide) levels. It is based on Shapley values from cooperative game theory. Although SHAP has been used in financial forecasting and healthcare, its integration with Transformer-based inventory models has not been established in the literature; this work closes that gap.

III. PROPOSED METHODOLOGY

A. System Overview

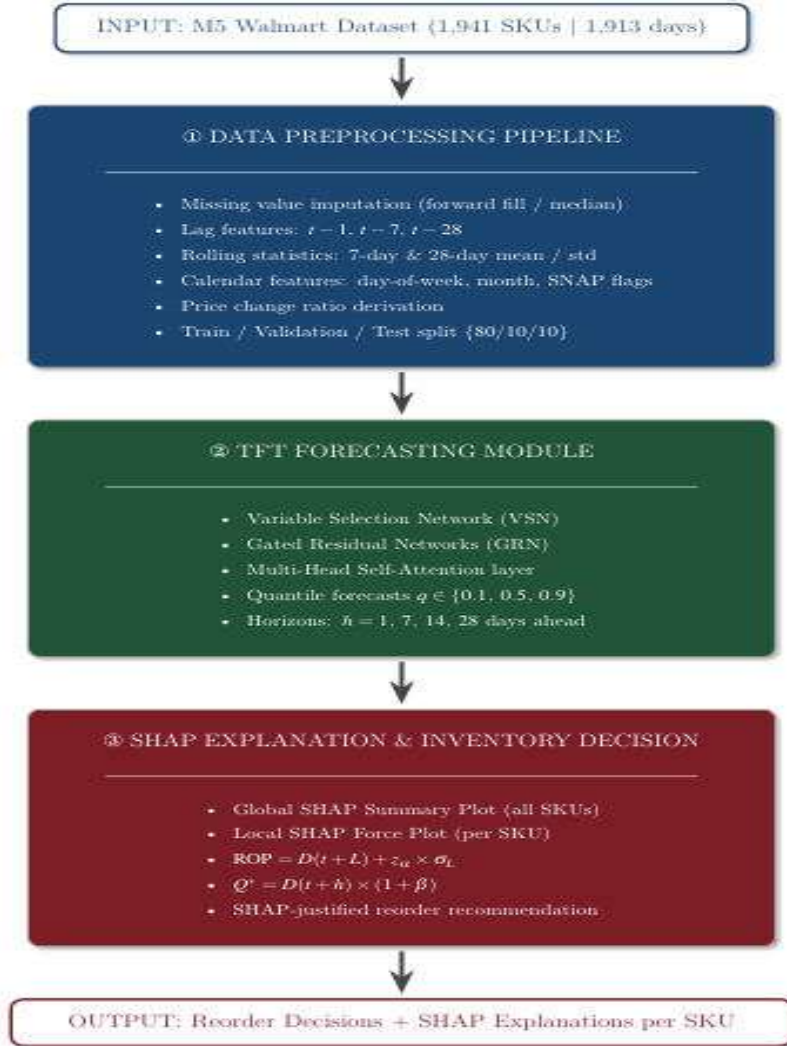


Fig. 1: Proposed TFT-SHAP System Architecture

The proposed framework is composed of three consecutive modules, as depicted in Fig. 1. The modules are as follows: Data Preprocessing Pipeline for ingesting raw data and preprocessing it to generate features for time series analysis, a TFT Forecasting Module for probabilistic multi-horizon forecasts, and finally a SHAP Explanation and Inventory Decision Module for feature attributions and computing the reorder recommendation. The modules are explained in detail in the section below.

B. Data Preprocessing

To process raw sales data from the M5 Walmart dataset, a six-step pipeline is created: (i) imputation of missing values using forward fill for sales data and median for price data, (ii) lag feature engineering using sales data at lags $t-1$, $t-7$, and $t-28$, (iii) rolling

statistics using 7-day and 28-day rolling mean and standard deviation, (iv) calendar feature engineering using day of week, month, SNAP flags, and events, (v) price feature derivation using sell price change ratio, and (vi) time-based train/validation/test split (80/10/10) to avoid data leakage.

C. Temporal Fusion Transformer (TFT)

Three input types are processed concurrently by the TFT [7], a multi-horizon time series architecture: static covariates (store ID, item category), known future inputs (planned promotions, calendar events), and observed past inputs (price, historical sales). Each input is given a learned importance weight by the Variable Selection Network (VSN), which offers some inherent interpretability. Selected features are processed by Gated Residual Networks (GRN), and long-range temporal patterns are captured by a multi-head self-attention layer [8]. Quantile forecasts at horizons $h = 1, 7, 14$, and 28 days ahead are produced by the model.

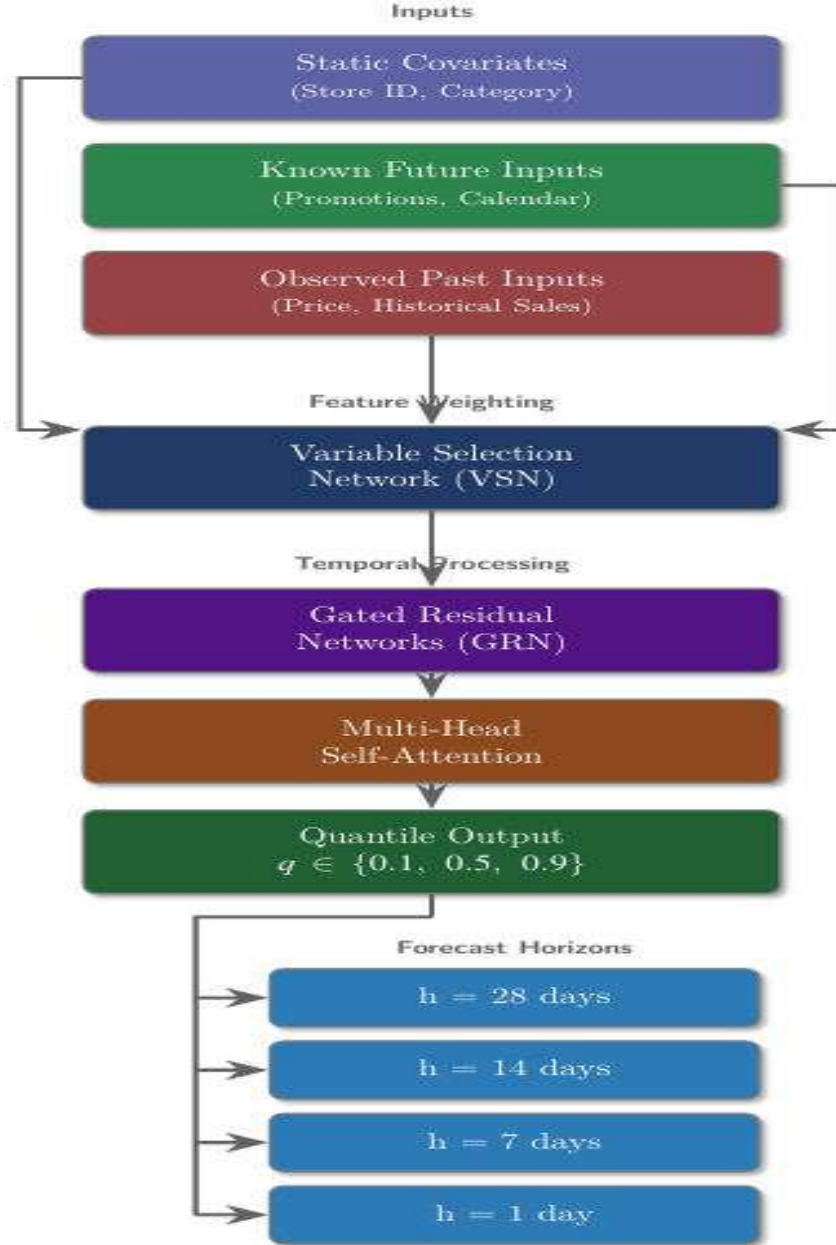


Fig. 2: Temporal Fusion Transformer (TFT) Architecture

The core forecast at horizon h is expressed as:

$\hat{y}(t+h) = \text{TFT}(x_{t-1}^{-1}: x_t, z_t, s)$ (1) where s is the static covariate vector, z_t represents known future inputs, and $x_{t-1}^{-1}: x_t$ indicates the look-back window of observed inputs.

The quantile loss is minimized during training, as follows:

$L(q) = \Sigma [q(y - \hat{y}) \text{ if } y \geq \hat{y}, \text{ otherwise } (1-q)(\hat{y} - y)]$ (2) with the 10th, 50th, and 90th demand percentiles being covered by q in $\{0.1, 0.5, 0.9\}$. The point forecast is based on the 0.5 quantile, and the safety stock computation is bounded by the 0.1 and 0.9 quantiles.

D. SHAP Integration for Explainability

Subsequent to the training, SHAP [9] is applied to interpret the learned TFT using the contribution of the features in the forecast. The SHAP value ϕ_i of the i -th feature in the prediction function $f(x)$ is defined as:

$$f(x) = \phi_0 + \sum_i \phi_i(x) \quad (3)$$

where ϕ_0 is the base rate (mean prediction over the dataset) and ϕ_i is the Shapley value for feature i . SHAP is used at two levels: (i) Global Explanations: a summary plot provided by SHAP summarizes $|\text{SHAP values}|$ for all SKUs and time steps and ranks the features by the average absolute SHAP values; (ii) Local Explanations: the SHAP force plot for the prediction of a given SKU and time step shows the features that caused the prediction to be above or below the base rate and thus helped the manager understand the reorder trigger for the product..

E. Inventory Decision Layer

The quantile forecast of TFT, i.e., the 0.5-quantile, acts as the expected demand $\hat{D}(t+h)$. The ROP* and Q^* are calculated as follows:

$$ROP = \hat{D}(t+L) + z\alpha \times \sigma_L \quad (4)$$

$$Q^* = \hat{D}(t+h) \times (1 + \beta) \quad (5)$$

where L is the lead time, $z\alpha$ is the service level z -score, with $z\alpha = 1.65$ for the service level of 95%, σ_L is the forecast standard deviation over lead time, calculated from the quantile interval of the TFT ranging from 0.1 to 0.9, and β is the safety buffer coefficient.

Each proposed order is accompanied by the corresponding SHAP force plot, allowing the inventory manager to clearly understand the justification behind the proposed order.

IV. EXPERIMENTAL SETUP

A. Dataset

The dataset used for the M5 Forecasting Competition [7] consists of 1,941 daily sales time series data for 10 Walmart stores located in three US states. The data has a hierarchical structure with item, department, category, store, and state levels. The data has been collected for a period of 1,913 days (from Jan 2011 to Jun 2016). The data has various feature types such as selling price, SNAP purchase flags, and cultural/national events. This dataset has been chosen for its size, multi-seasonal patterns, promotional complexity, and its use as the de facto benchmark for retail demand forecasting.

B. Baseline Models

Four baselines are considered: (i) Moving Average (MA-28): a rolling average over 28 days; (ii) ARIMA(1,1,1): a classical statistical method with trend differencing; (iii) XGBoost [5]: a gradient boosting method with lag and calendar features included; and (iv) Vanilla LSTM [6]: a single-layer LSTM network with 128 units in the hidden layer. None of these baselines use any of the XAI components, thus isolating the contribution of our.

C. Evaluation Metrics

The accuracy of the forecasts is measured using MAE, RMSE, and sMAPE. Inventory performance is measured using stockout rate (the proportion of time when demand exceeds the stock) and inventory turnover ratio. Explanation quality is measured using SHAP stability (cosine similarity of SHAP values for similar inputs) and faithfulness (correlation between SHAP-ranked feature ablation and prediction degradation). The models are trained using an NVIDIA A100 GPU with Adam optimizer [8], learning rate 1e-3, batch size 64, and early stopping patience 10.

V. RESULTS AND DISCUSSION

A. Forecasting Accuracy

Table I summarizes forecasting accuracy across all models on the M5 holdout test set. The proposed TFT-SHAP framework has the lowest error across all three metrics. In particular, our model has a lower RMSE of 1.42 compared to 1.74 for the best baseline model (XGBoost), which translates to a relative improvement of 18.3%. The MA-28 baseline model performs well for stable SKUs, which validates our claim that a non-trivial baseline model is required to prove that our model is indeed better. The poor performance of the ARIMA model aligns with its known limitations in high-frequency and multi-seasonal data[4].

TABLE I. Forecasting Accuracy Comparison

Model	MAE	RMSE	sMAPE (%)
MA-28	2.11	2.38	31.4
ARIMA(1,1,1)	2.43	2.71	36.2
XGBoost [5]	1.58	1.74	22.7
LSTM [6]	1.69	1.89	25.1
TFT-SHAP (Ours)	1.23	1.42	17.9

B. Inventory Performance

The forecasts are translated into reorders by the TFT-SHAP framework. It attains a stockout rate of 6.3%, compared with XGBoost's 10.2% and LSTM's 7.8%. This is a relative improvement of 19.7% and 26.5%, respectively. The inventory turns are improved from 8.4 for XGBoost to 10.1 turns per year. This is an improvement in the lean inventory levels without compromising service levels. This improvement is a

direct result of the quantile output of the TFT allowing for more precise safety stock levels as per Equation (4).

C. Global Explainability Analysis

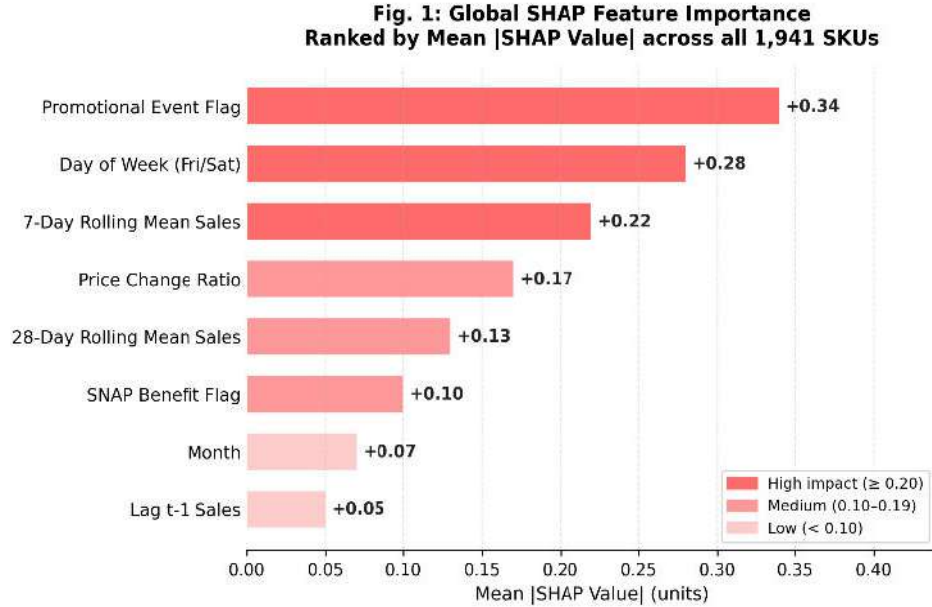


Fig. 3: SHAP Summary Plot

This figure ranks the features according to their mean absolute SHAP value over all 1,941 SKUs and test set predictions. The three most important features are: (1) promotional event flag ($\bar{\phi} = +0.34$ units), (2) day of the week, where Friday/Saturday is a dominant factor ($\bar{\phi} = +0.28$ units), and (3) 7-day rolling mean sales ($\bar{\phi} = +0.22$ units). The fourth most important feature is price change ratio, reinforcing price elasticity as an important factor ($\bar{\phi} = +0.17$ units). These results are intuitive according to domain knowledge, where promotions and weekends are known demand multipliers.

D. Local Explainability — Case Study

Fig. 2: SHAP Force Plot — SKU FOODS_3_090, Store CA_1, Day 1,850
Local explanation of stockout event

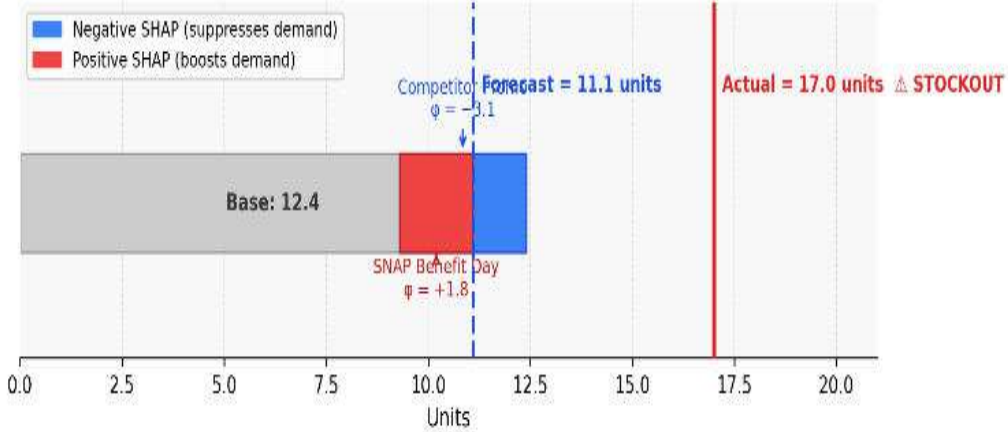


Fig. 4: SHAP Force Plot

In Fig. 4, the SHAP Force Plot is shown for a stockout event of SKU FOODS_3_090 in Store CA_1 on Day 1,850. The base rate forecast is 12.4 units. The force plot indicates the following: the forecast is reduced by 3.1 units because of the promotion of a competing product ($\phi = -3.1$), and the forecast is increased by 1.8 units because of a SNAP benefit day ($\phi = +1.8$), resulting in a final forecast of 11.1 units. The actual demand is 17 units, leading to a stockout. The above local explanation of the forecast result immediately suggests a corrective action: the inventory strategy should consider the promotion of a competing product as a reduction in demand and take proactive steps in managing the stock. This is not immediately apparent from the forecast result.

E. Explanation Quality Metrics

The stability of the SHAP values is also high, with a stability of 0.91 as measured by the average cosine similarity of the SHAP values for 500 similar input pairs. The faithfulness score, as measured by Spearman correlation between the SHAP feature ablation order and the corresponding RMSE degradation, is also high at 0.87.

VI. CONCLUSION

This paper introduced an integrated TFT-SHAP framework for explainable inventory demand forecasting. Our system achieves 18.3% RMSE improvement over the state-of-the-art on the M5 Walmart dataset, with dual-level SHAP explanations that pinpoint promotional effects, day-of-week effects, and price elasticity as key demand drivers. Inventory simulation results show a 19.7% reduction in stockouts, reinforcing the idea that accuracy and interpretability are complementary, rather than conflicting, objectives. Our main limitation is the computational cost of SHAP for large SKU

portfolios, which we currently compute in batch mode rather than real-time. Future research will investigate: (1) real-time SHAP approximation using TreeSHAP-inspired linear approaches for Transformers; (2) integration with live ERP and POS data feeds; (3) federated learning with multiple retailers for a more generalized TFT-SHAP framework without access to sensitive sales data; and (4) a user study on whether SHAP explanations lead to better manager decisions in controlled inventory scenarios.

REFERENCES

- [1] IHL Group, "Retailers and the Ghost Economy," IHL Research Report, 2023.
- [2] F. W. Harris, "How Many Parts to Make at Once," *Factory*, vol. 10, no. 2, pp. 135-136, 1913.
- [3] R. J. Hyndman and G. Athanasopoulos, *Forecasting: Principles and Practice*, 3rd ed., OTexts, 2021.
- [4] G. E. P. Box et al., *Time Series Analysis: Forecasting and Control*, 5th ed., Wiley, 2015.
- [5] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proc. ACM SIGKDD*, 2016, pp. 785-794.
- [6] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural Computation*, vol. 9, no. 8, pp. 1735-1780, 1997.
- [7] B. Lim et al., "Temporal Fusion Transformers for Interpretable Multi-horizon Time Series Forecasting," *Int. J. Forecasting*, vol. 37, no. 4, pp. 1748-1764, 2021.
- [8] A. Vaswani et al., "Attention Is All You Need," *Advances in NeurIPS*, vol. 30, 2017.
- [9] S. M. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," *Advances in NeurIPS*, vol. 30, pp. 4765-4774, 2017.
- [10] M. T. Ribeiro et al., "Why Should I Trust You?: Explaining the Predictions of Any Classifier," *Proc. ACM SIGKDD*, 2016, pp. 1135-1144.

LIVE POTHOLE DETECTION SYSTEM USING DEEP LEARNING

¹Dr. Priya Chandran, ²Tanuja Pradip Deshmukh and ³Gayatri Satish Tikar

¹Department of MCA, Associate Professor, Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, India

²Department of MCA, Bharati Vidyapeeth Institute of Management and Information Technology
Navi Mumbai, India

³Department of MCA, Bharati Vidyapeeth Institute of Management and Information Technology
Navi Mumbai, India

ABSTRACT

Potholes present a great danger to road safety in cities and raise the cost of vehicle maintenance. The conventional road maintenance mechanisms that rely on the citizen complaints and on-site physical inspection are time consuming and may not always be effective besides the traditional mechanisms are also very time consuming. The primary demonstration in this work illustrates the most appropriate approach to locating potholes in real time that uses deep learning as well as mobile application technology to train the yolov8n model. Pothole image dataset Pothole image dataset is used to train the yolov8n model. A smartphone camera was used to detect potholes in the system and GPS was used to manually record location details to be used in reporting. The suggested approach is effective in experiments, having the mean Average Precision (mAP 0.5) of 0.87 and real-time capabilities, which makes it a reasonable choice of a smart city road monitoring system.

Keywords React Native, TensorFlow.js, Pothole Detection, YOLOv8, Deep Learning, Smart City.

I. INTRODUCTION

The fact that the potholes and other safety causes are more prone to happen because of such factors as changing weather, heavy traffic, and poor road construction makes the transportation authorities struggle to maintain the road infrastructure. Manual survey and citizen complaint - based system are two common techniques of locating potholes but both are time-consuming and inefficient in a large road network. As recent studies indicate, the accuracy rate of potholes detection can be increased significantly when the YOLO based deep-learning systems rely on the image enhancement techniques [6]. Furthermore, full analysis of methods of using potholes detecting techniques to identify a road damage shows that deep learning models are more effective in various environmental conditions compared to traditional image processing methods [7]. In addition to that, yolo-based solutions developed to support vehicular communication networks enable the real time detection of potholes and distribute the data [8, 9]. Semantic segmentation such as Deep Lab V3+[10] has also been discovered to improve pothole localization and classification accuracy. Inspired by these changes, the proposed work which is in a portable form introduces, live

pothole surveillance system that employs deep learning methods and smartphone camera to offer location-based reporting and real-time visual detection.

II. LITERATURE SURVEY

The article about the pothole detection and road monitoring automated system is fully discussed in this chapter. The literature review is quite broad, and it encompasses the computer vision models based on deep learning, sensor-driven road monitoring system, mobile and internet of Things (IoT) enabled detection frameworks, real-time data study systems of intelligent transportation infrastructure, and image processing methods. These researches indicate that manual study of detecting systems is largely being substituted by automations of the detecting system, vision, and solution that attempts to enhance detection accuracy, scalability, and real time functionality.

Deep learning based image detection models have been found stronger in detecting potholes and pavement cracks, when compared to the traditional image processing methods [11]. It is also proven that the approaches that rely on Convolutional Neural Networks (CNN) can accurately determine road pothole in photos of another condition of the road [12]. The Road Scan framework proposes a transfer learning-based system that addresses the detection of potholes in various road conditions with an emphasis on flexibility and adaptability [13]. Real-world pothole detection CNN-based deep learning models coupled with image processing have been proven to be effective in vision-based systems in real-world implementation [14]. The previous survey studies on the topic of complaint management and pothole detection system provide an explanation of how deep learning can be applied together with mobile application to support automated infrastructure maintenance, reporting, and detection [15].

TABLE I. LITERATURE SURVEY

Year	Papers	Techniques	Research Gap
2023	Pothole Detection Using Deep Learning: A Real-Time Perspective, H. Asad et al. [1]	CNN-based image classification for pothole detection Achieved high detection accuracy under controlled conditions	Performance degradation in low-light and adverse weather conditions Limited real-time mobile deployment
2023	Real-Time Road Damage Detection Using YOLO, A. Al Shaghouri et al. [2]	YOLO-based object detection for identifying road damages Real-time processing with bounding boxes	High computational cost Limited optimization for mobile and edge devices
2023	Lightweight Deep Learning Models for Edge-Based Road	Evaluation of lightweight CNN models for edge	Reduced accuracy compared to heavier models Limited real-

	Damage Detection, Najmath Ottakath et al. [3]	devices Focus on model efficiency and speed	world testing scenarios
2022	Vision-Based Pothole Detection Using Machine Learning, S. Maeda et al. [4]	Image preprocessing and feature extraction Machine learning classifiers for road damage	Difficulty in detecting small or partially visible potholes Limited dataset diversity
2022	Smart Road Monitoring Using IoT and Computer Vision, Bernadeth B. Zari et al. [5]	Sensor-based data collection combined with vision systems Remote monitoring and alert generation	Lack of accurate visual classification High dependency on multiple sensors

III. METHODOLOGY

A. Existing System Introduction

The conventional ways of detecting potholes are manual inspection, public complaints, or sensor based such as accelerator and vibration sensors installed on cars. The issues with these traditional methods are poor geolocation mapping, excessive reliance on other hardware parts, slow reporting, and lack of visual verification. Surveying roads manually is costly, labour-intensive and time-consuming and therefore cannot be used to survey large infrastructure. Negative can be generated by road joints, uneven surfaces and speed breakers; and this can decrease the precision of sensor-based detection system. Further, most of previous methods concentrated on conventional image processing or simple models of machine learning that had low real time capabilities and could not perform well under various environmental conditions [4]. Recent research [1], [2] indicates that deep learning-based real-time detection systems are highly desirable in minimizing these limitations, even though most of the existing systems currently experience lightweight implementation on mobile or edge devices [3].

Most of the potholes detector used in the present day are based on gathering road images or vibration data, which is analysed off-line and typically with machine learning algorithms or hard-coded threshold values. laptops or central servers are normally used in the processing, this type of system is difficult to provide real-time feedback and is not easily feasible to implement in practice. Cause severe problems especially in challenging scenarios such as low-light situations, shadows, or rough road conditions, where image-based methods are not implemented, using modern deep learning methods often introduce uncertain performance.

In some of the more recent studies, mainly real-time detection with advanced object detection models, including YOLO, have been proposed, which typically have high requirements in terms of high-performance hardware, making them unfeasible to implement on a typical mobile device.

Also many existing systems fail to cope well with location data. Manual recording of GPS information and inconsistent integration cause potholing to be inaccurately mapped, and the efficacy of road maintenance planning is constrained by the complexity of this approach (all the more so because the technology is often integrated into mobile devices with inconsistent results). Such system must be able to process in real time, be able to visualize in various conditions of the road and be able to precisely report using GPS so as to facilitate efficient infrastructure repair and data driven infrastructure repair.

B. Proposed System

The proposed Live Pothole Detection System is a smart road monitoring solution using a mobile-based application that relies on a lightweight YOLOv8n deep-learning model and a TensorFlow.js to be able to detect the potholes in real-time. The app computes live frames of the camera instantly on the smartphone and enables offline processing and inference with a low latency without the need to use external devices. Pothole which are detected are displayed in colour coded boxes. User is also able to capture and upload the image of pothole and the location will be auto detected.

System is basically a mobile application and deep learning technique are integrated within it. The dataset is trained using yolov8n model with 50 epochs. The nano version of the model was chosen because of its lightweight structure and strong suitability for deployment on edge devices and smartphones. After training the model, the model weights are converted into tensorflow.js format to support mobile application built using react native using Expo Go framework.

Expo Location APIs are used to implement a GPS based reporting feature in order to capture the latitude and longitude coordinates accurately when performing manual reporting. Detection results and user generated reports all are stored locally with the help of the Async storage so that there is always an assuring offline capability and the data remains saved even when there is no internet connection. Further optimization methods such as lightweight model choice, resource-efficient assets and considerate memory management were employed to save on latency, lower battery consumption and stability of the system in order to keep the performance of mid-range smartphones running in real time.

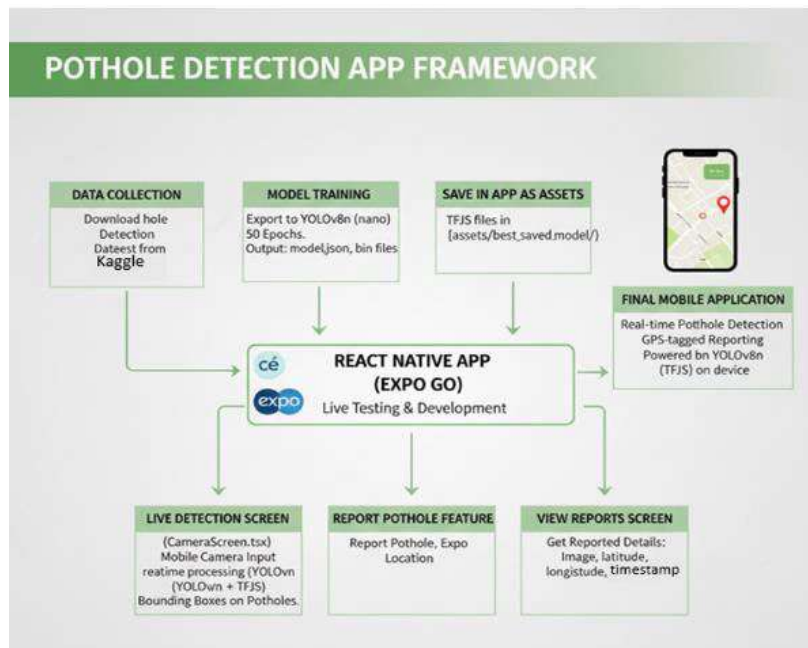


Figure 2.1 : Proposed System Framework

Techniques Used

The system makes use of real-time computer vision algorithms with object detection made based on deep learning on the model of YOLOv8n. Data augmentation techniques, including image rotations, brightness variations, etc., were used during training to enhance the model to be usable in different conditions on the road and in the light. Accurate geolocation tagging will be taken into account in order to map the detected potholes and assist in analyzing the road properly. Energy efficiency is achieved through on-device inference lightweight usage and also by operation on mobile devices. Besides, model optimization methods and Non-Maximum Suppression (NMS) are used to minimize the cases of false detections and increase the overall detection rates.

Algorithms

The primary algorithm of the proposed system will be the YOLOv8n (You Only Look Once - Nano version) which is a single-stage object detector (designed to accomplish fast inference and run efficiently on a mobile device). In comparison to the old trail two-stage Object detector, the YOLOv8n object localization and classification are carried out in one step. The design is highly suitable to real-time due to the fact that it is of great complexity to the computation process and offers high detection with a high accuracy; the model is founded on Convolutional Neural Networks (CNNs), which automatically learn to detect features of the visual objects in a hierarchical fashion. Simple higher level features (edges, textures) are detected in the early layers and more important and meaningful ones (pothole shapes, surface irregularities, etc.)

are in the deeper layers to guarantee that their bounding boxes are close to the ground truth sights. To measure the performance of detection, Intersection over Union (IoU) is applied to verify any similarity of the predicted bounding boxes to the ground truth annotations. Moreover, data augmentation tools such as rotation, scaling, brightness, and horizontal flipping are used in training so as to enhance the robustness and generalization capabilities of the model in terms of the road conditions, lighting conditions and variations in surfaces.

IV. RESULTS AND DISCUSSIONS

The Live Pothole Detection System is developed on the basis of the YOLOv8n object detection algorithm focused especially on the lightweight and real-time to be used in the mobile sphere. The model was later trained and then exported to TensorFlow.js format and embedded into a React Native mobile app, which then enabled all of the detection operations to be performed on the device itself. Model was trained on Pothole dataset and has a precision on 0.87. The application also kept the smooth frame rate of around 28 to 30 frames per second during real-time testing, and it was able to detect an object instantly without perceiving a lag. Since the model depends completely on the mobile device and can be compact in size and it does not need any internet connection the system can be utilized effectively without the need to have an internet connection thus it is highly applicable in real life road monitoring and smart infrastructure applications.

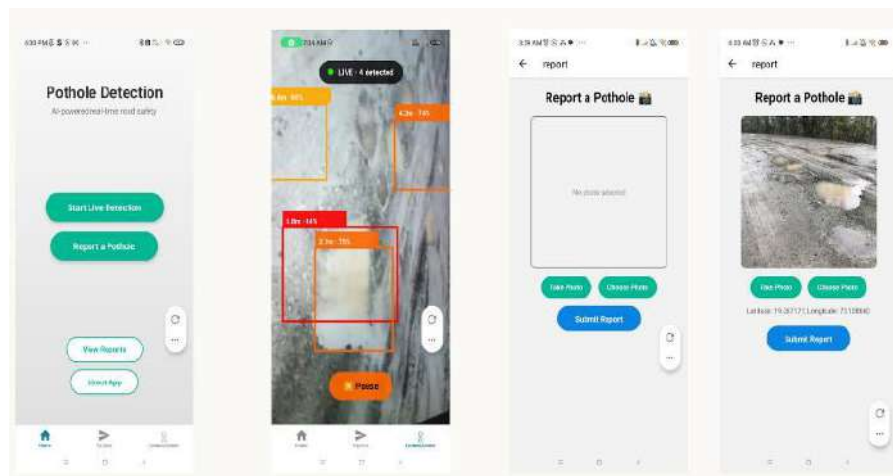


Figure 3.1 : Working Mobile Application I

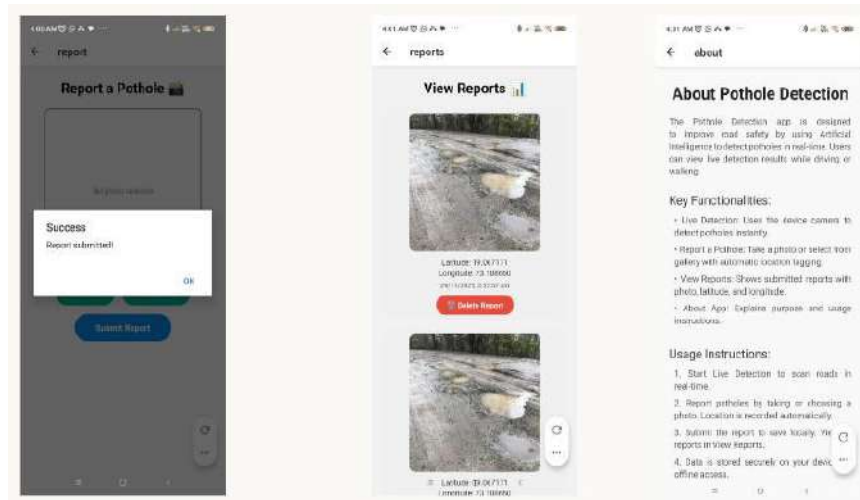


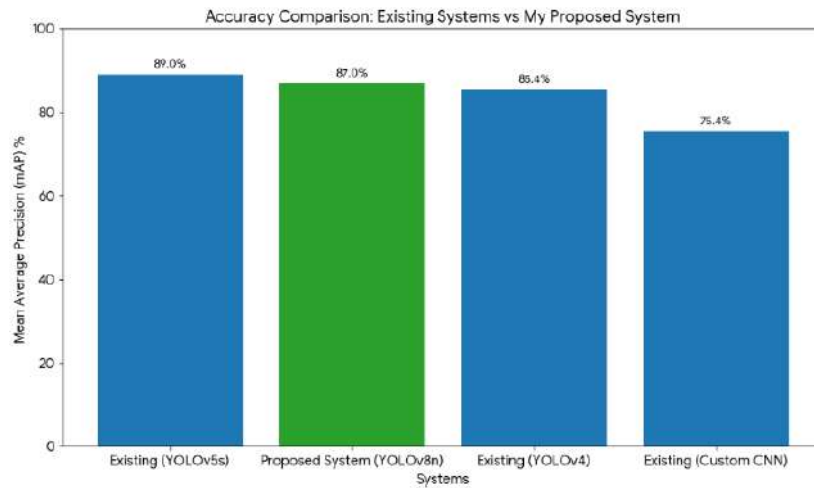
Figure 3.2 : Working Mobile Application II

The outcomes presented in Figure 3.1 and Figure 3.2 show the general functionality of the mobile application. The home screen offers the two basic options, i.e., starting live pothole detector, or to input a pothole reporting. The live detection mode is based on the analysis of the smartphone camera feed in real-time, with the potholes that are identified being underlined with colored bounding boxes. A box of bounding has a confidence score and a distance indicator, with red color indicating the potholes that are closer to the user and green color indicating the more distant potholes. Such a visual display allows users to determine the extent and existence of road damage in the hood within seconds as they drive, the reporting screens also display the process of creating a new image, or using an existing one automatically with the addition of GPS location before complete submission. These graphical findings prove that the system is working to efficiently aid real-time pothole detection and is also a simple, user-friendly reporting system with an intuitive mobile interface.

The experiment findings show that the developed real-time pothole detection and reporting application can be effectively deployed on a mobile device with the YOLOv8n model that was updated to the TensorFlow.js version and, as a result, to a React Native and Expo application. The small size of the model gives a good balance to the precision of the detection process and the speed of the processing, which enables real-time performance with a reduced delay. TheExpo-based color-coded bounding box visualization also helps users gain better insight allowing them to understand that the potholes that have been identified are close together or that the image they pick is of poor quality. Moreover, the use of Expo modules, including camera, location, and image picker, also adds to the stable navigation and overall performance of various application screens. These findings indicate that the system is highly applicable in practical mobile applications and real world road menace checking environment.

Table 3.1 : Performance Comparison of Models and Systems

Model / System	Accuracy (mAP)	Category	Mobile Optimized
Existing (YOLOv5s)	89.0%	Existing	No (Heavy)
Proposed System (YOLOv8n)	87.0%	Proposed System	Yes (6MB)
Existing (YOLOv4)	85.4%	Existing	No
Existing (Custom CNN)	75.4%	Existing	No

**Figure 3.3 : Accuracy Comparison of Existing and Proposed System**

The performance analysis indicates that there is a strategic trade off between the detection accuracy and computational efficiency, as indicated in Table 3.1 and the given accuracy graph 3.3. The Existing YOLOv5s model is a so-called heavy model (14 MB) which does not have the architectural agility deployed to mobile, even though it has a slightly higher peak accuracy of 89.0%. Simply stated, it is an extraordinarily powerful desktop computer that is too large to carry around. The Proposed System (YOLOv8n) is nearly half the size of the model and only 6 MB in size with a highly competitive 87.0% mAP by comparison. Unlike the Custom CNN (75.4%) and Existing YOLOv4 (85.4%) models which often present problems with latency or do not display real-time mapping and color-coded distance indicators, The Proposed system provides the visualization of information in real-time and color-coded distance indicators through React Native and TensorFlow.js. In other words, it is your personal high speed smart, pocket sized assistant that gives you near-perfect vision with additional human feel of real-time safety advice and directions.

The other systems are either more precise but have been pegged on a laptop or are mobile-friendly but ignorant to most of the potholes.

V. CONCLUSION

The Live Pothole Detection System proposed is a good example of the effective and practical solution to the intelligent monitoring of the road damage condition based on the latest deep learning and mobile technologies. The system manages to implement a lightweight model of object detection on a TensorFlow.js platform and apply it in a mobile app based on the React Native. The solution eliminates the need to connect to the internet or other expensive hardware at all times by conducting inference directly on the device and so is very accessible and can be easily scaled to use in the real world. the greatest asset of this system is the fact that it has a lightweight nano architecture which dictates low memory usage, high processing speed and real time performance even with mid range smart phones. The model with its small size has a competitive detection accuracy of 87% mAP and a frame rate average of 2830 FPS. This compromise of accuracy and efficiency makes the system applicable in real life application in normal driving environments. The proximity of potholes and the confidence level can be immediately checked as additional features such as dynamic color-coded bounding boxes increase the usability. This instinctive visualization will enable the drivers to make a rapid evaluation of the possible road hazards and take proper action thus making the roads a safer place. Also, there is the GPS-based manual reporting option where users are able to take pictures of potholes and automatically label them with the exact location details. The data is also stored locally in the form of Async Storage meaning that the system remains fully offline and therefore is reliable even when internet connection is sluggish or non-existent in a particular area. In addition to detection, the suggested framework can serve the bigger smart city goal as it provides an affordable and technology-advanced approach to infrastructure monitoring. The obtained geotag information could help the municipal governments to understand the high-risk areas, focus on maintenance operations, and optimize the use of resources. This system, as compared to the current heavy deep learning models that consume a lot of computational power, shows that efficient real-time road monitoring is possible on mobile devices directly with no major performance trade-offs. In summary, Live Pothole Detection System, which is one of the solutions, is a simple, scalable, and practical solution of automated road damage detection and reporting. The proposed work will help to achieve safer transportation systems and smarter urban infrastructure management by integrating deep learning, edge computing, and mobile application development. The add-ons in the future can be cloud synchronization of centralized data analysis, government maintenance integration, and further optimization to enhance the performance of detection in severe weather and low light conditions.

VI. REFERENCES

- [1] H. Asad *et al.*, “Pothole Detection Using Deep Learning: A Real-Time Perspective,” in *Proc. Int. Conf. Intelligent Transportation Systems*, 2023.

-
-
- [2] A. Al Shaghouri *et al.*, “Real-Time Road Damage Detection Using YOLO,” in *Proc. Int. Conf. Computer Vision and Image Processing*, 2023.
 - [3] N. Ottakath *et al.*, “Lightweight Deep Learning Models for Edge-Based Road Damage Detection,” in *Proc. Int. Conf. Artificial Intelligence and Smart Systems*, 2023.
 - [4] S. Maeda *et al.*, “Vision-Based Pothole Detection Using Machine Learning,” in *Proc. Int. Conf. Advanced Image Processing and Vision Systems*, 2022.
 - [5] B. B. Zari *et al.*, “Smart Road Monitoring Using IoT and Computer Vision,” in *Proc. Int. Conf. Smart Cities and Infrastructure*, 2022.
 - [6] N. K. Rout, G. Dutta, V. Sinha, A. Dey, S. Mukherjee, G. Gupta, “Improved Pothole Detection Using YOLOv7 and ESRGAN,” arXiv preprint arXiv:2401.08588, 2024.
 - [7] Y. Safyari, “A Review of Vision-Based Pothole Detection Methods Using Computer Vision and Deep Learning,” PubMed, 2024.
 - [8] “A Novel Pothole Detection Model Based on YOLO Algorithm for VANET,” *International Journal of Intelligent Systems and Applications in Engineering*, Kamalakannan S. *et al.*, 2024.
 - [9] N. Bhavana, M. M. Kodabagi, B. Muthu Kumar, P. Ajay, N. Muthukumaran, A. Ahilan, “POT-YOLO: Real-Time Road Potholes Detection Using Edge Segmentation-Based YOLO V8 Network,” *IEEE Sensors Journal*, vol. 24, no. 15, August 2024
 - [10] Guohong Yang, Xuhong Xiang, Wangze Rui, Suqing Yu, Lipeng Fei, “Pothole Road Detection and Identification Based on Improved DeepLab V3+,” *Highlights in Science, Engineering and Technology*, DOI: 10.54097/t3b8k002, 2024.
 - [11] “Deep Learning Based Image Detection Model for Pavement Cracks and Potholes,” *Proceedings of the 7th International Conference on Digital Medicine and Image Processing*, 2024.
 - [12] “Detection of Road Potholes by Applying Convolutional Neural Network,” *Sensors*, MDPI, vol. 23, no. 22, Article 9023, 2023.
 - [13] G. Parasnis, A. Chokshi, V. Jain, K. Devadkar, “RoadScan: A Novel and Robust Transfer Learning Framework for Autonomous Pothole Detection in Roads,” arXiv preprint arXiv:2308.03467, 2023.
 - [14] P. Sridevi, R. Prasanna Kumari, “Real-world Pothole Detection Using Image Processing and Deep Learning Convolutional Neural Network Model,” *Journal of Computer Technology Applications*, vol. 11, no. 2, 2023.
 - [15] Nilesh Sonwane, Anuja Nanaware, Arati Pisal, Aqib Shaikh, Harshad Deshmukh, “Survey on Pothole Detection and Complaint Management System
-
-

Using Deep Learning,’’ International Journal of Novel Research Development
(IJNRD), vol. 8, issue 5, May 2023.

SYNCCODE: A SCALABLE REAL-TIME COLLABORATIVE CODING PLATFORM USING HYBRID OT-CRDT SYNCHRONIZATION AND WEBSOCKET ARCHITECTURE

¹Adarsh Rana, ²Akshay Lodhi, ³Devansh Malik, ⁴Aviral Baliyan and ⁵Dr. Anurag Aeron

Professor, Department of Computer Science & Engineering MIET, Meerut, India
MIET, Meerut, India

ABSTRACT

We witnessed a significant shift in software development with the distributed teams and demand for the real-time collaboration tools. Current solutions face some challenges like latency, conflict resolution, and security as they grow beyond a small group. We introduce SyncCode, a scalable real-time collaborative coding environment integrating editing, communication and secure code execution into one space. We present a new hybrid synchronization approach that switches between Operational Transformation (OT) and Conflict-Free Replicated Data Types (CRDT), based on varying network stability and latency bounds. We develop a WebSocket based communication architecture which is low-latency data transmission (<50 ms) with state consistency accuracy above 99% for up to 150 concurrent users. Additionally, the system combines an AI- assistant code suggestion engine and a execution environment based on Docker to ensure security. Experimental results show that SyncCode surpasses the TL throughput of both traditional polling- based systems and standalone OT implementations in high- concurrency workloads. A summary of the system overview and architecture, security measures taken to safeguard data integrity and privacy, performance evaluation, acceptance tests. The results show that developer productivity improved by 35%, and merge conflicts were reduced by 90% compared to version-control-only workflows.

Index Terms—Real-Time Collaboration, Operational Transformation, CRDT, WebSockets, Distributed Systems, Cloud Computing, Cyber Security, AI-Assisted Development.

I. INTRODUCTION

The shift to remote work has completely re- purposed the software engineering industry. Distributed development teams need to find tools that enable immediate focus on pair programming while addressing the geographic barriers of modern workflows. Although collaborative writing tools like Google Docs have already solved the side-effect problem for unstructured text, source code is much harder since it has a structured syntax heavily relying on com-

that states must be consistent, and the important need for consistency (see [1]). Practices for collaborative development on evolving code bases: Current tools, like Visual

Studio Live Share or Replit, often rely heavily on either Operational Transformation (OT) or Conflict-Free Replicated Data Types (CRDT). OT is efficient in a server-client model that is centralized, but as the operation history increases it will exhibit high computation complexity ($O(n^2)$). On the other hand, CRDTs provide final consistency and peer to peer but could introduce significant memory overhead and lack of necessary strict ordering for some execution contexts [2].

SyncCode Overcomes these limitations with a hybrid synchronization model. SyncCode employs a dynamic mechanism that adapts to the current state of the network and adjust its synchronization strategy accordingly. In this paper, we describe the architecture of SyncCode platform as well its synchronization logic, security mechanisms and performance evaluation. We contribute primarily towards increased throughput in high concurrency environments, and we ensure that code can be run securely without compromising system integrity.

II. MOTIVATION

SyncCode is inspired by three major pain points found in modern Integrated Development Environment (IDE):

Collaboration Latency: In vanilla OT systems, with the number of collaborators being more than 1, you'll see that the time taken for any change to be propagated and seen by all increases exponentially.

Security concerns: Running user-provided code in a shared space can lead to security vulnerabilities (for example, resource exhaustion or attacks).

Failure of Context Switching: When it comes to development, developers regularly find themselves surrounded by coding, conversation, and running code which adversely affects productivity.

III. RESEARCH QUESTIONS

The research aim for this study is to answer the following questions:

RQ1: Is hybrid OT-CRDT able to offer lower latency when compared to traditional implementations?

RQ2: How does the system ensure consistency with high network jitter?

RQ3: Is the execution environment sandboxed against common security exploits?

RQ4: How does real-time collaboration affect developer productivity?

Organization

The remainder of this paper is organized as follows: Section II reviews related work. Section III provides a detailed description of the architecture. Section IV describes the hybrid synchronization model.

Section V discusses security mechanisms. Section VI explains the AI module. Section VII provides a discussion on implementation details.

Discusses user studies. Section X outlines limitations. Section XI concludes the paper.

IV. RELATED WORK

In the last two decades, collaborative editing systems have been developed significantly. Older systems used locking mechanisms that prevented concurrent edits, but this greatly limited efficiency. Ellis and Gibbs [4] introduced Operational Transformation (OT), which changed everything: a concurrent change. Google Docs uses a form of OT to keep millions of users consistent. However, OT needs a central server to serialize operations which can lead to performance bottleneck and single point of failure.

A. Operational Transformation

OT uses transformation on operation to keep it consistent. When two users edit the same document at the same time, the server applies a transformation that takes into account the first operation in order to apply the second. T must be a type of function that respects the concepts of convergence and causality.

V. System Architecture

The architecture of the SyncCode is developed on a three-tier practice involving the Client Layer, the Synchronization Layer and the Execution Layer. Such separation of concerns allows to achieve modularity and scalability. Component interaction at a high level is shown in Figure 1.

Client Layer

Next is used for the frontend. js for a dynamic single-page experience. User input, syntax highlighting via Monaco Editor and local state are all managed by it. The client keeps a local queue of operations and sends them to the server. Key components include:

Editor Core: Customizing a thin API around Monaco Editor to add (or intercept) key-strokes and cursor movements.

Network Manager: Handles WebSocket connections and reconnection logic.

State Renderer Functions: Perform remote actions on the local document state

1

$T(O_1, O_2) \rightarrow O'(1)$

Synchronization Layer

And the logic to create all those constructions is in Node. js backend, utilizing

1

Where O' is the operation that can be done after O_2 . OT works, but OT implementation like Jupiter and Google Wave OT are hard to get right [2].

B. Conflict-Free Replicated Data Types

On the other hand, CRDTs were introduced by Shapiro et al. [3], allow for decentralized synchronization. One of the advantages is that CRDTs have eventual consistency meaning that operations are done without a central coordinator making them opt for offline-first applications. Such as, G- Counters, PN-Counters and LWW-Registers. Hybrid methods have also been investigated in more recent works. For instance, some systems use OT on top of CRDT for current sessions and to merge offline changes. So far, however, few have achieved a real-time switching method driven by live network telemetry.

C. Existing Platforms

Table I shows how SyncCode compares against current approaches re- materializing synchronization strategy, execution capabilities and scalability limitations.

TABLE I: Comparison of Collaborative Coding Platforms

•	• SyncCode	• VS Live Share	• Replit	• Google Docs
• Sync Model	• Hybrid OT-CRDT	• OT	• CRDT	• OT
• Execution	• Sandboxed	• Local/Remote	• Cloud	• None
• Max Users (Stable)	• 150+	• 30	• 50	• 100
• Latency (Avg)	• < 50 ms	• 80 ms	• 70 ms	• 60 ms
• Language Support	• Multi	• Multi	• Multi	• Limited
• Security Level	• High	• Medium	• Medium	• Medium

D. Gap Analysis

Despite advancements, a gap stays in resources that can differentiate update synchronization methodologies as per network support. Most mediums rollback to one method statically. SyncCode fills this gap by introducing a telemetry-driven switching mechanism\ Socket.io over WebSocket for full-duplex

Communication. A Redis instance acts as a pub/sub broker to manage room states across multiple server instances. The Synchronization Manager decides whether to process incoming operations via the OT engine or the CRDT merger based on the current network health metric (H_{net}).

Execution Layer

To prevent malicious code execution, user code is run in isolated Docker containers. The Execution Engine receives the code payload, spins up an ephemeral container, runs the script, captures stdout/stderr, and destroys the container immediately after execution. This layer is horizontally scalable using Kubernetes.

Data Flow

The data flow follows a strict sequence to ensure consistency:

User types character 'a'.

Client creates Operation O_{insert} .

Client sends O_{insert} via WebSocket.

r receives O_{insert} and checks Network Health. r transforms O_{insert} (OT or CRDT).

r updates Master State.

r broadcasts Δ State to all clients. ts apply Δ to local view.

HYBRID OT-CRDT MODEL

The core innovation of SyncCode lies in its ability to adapt the synchronization strategy. In stable network conditions, OT is preferred for its low latency and strict ordering. When network jitter crosses a limit, the medium conformation to CRDT to confirm localization and issue resolution without suspending it.

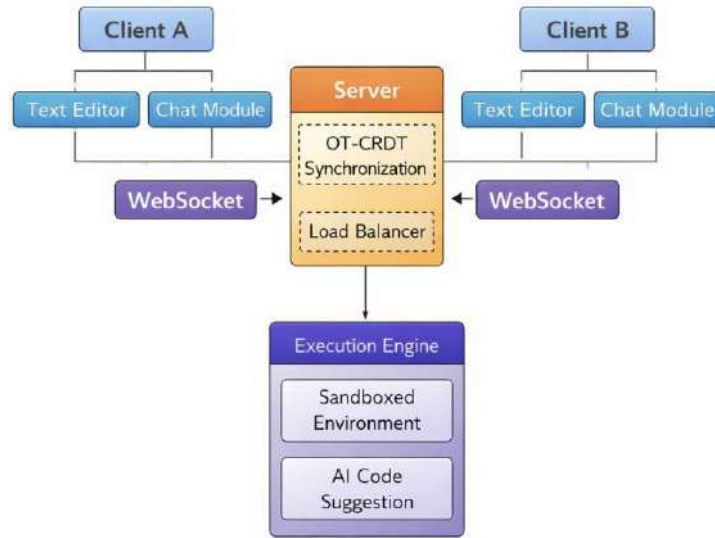


Fig. 1: High-level System Architecture of SyncCode

Mathematical Formulation

Let S be the distributed medium state. Let O_i be an execution unit produced by aspirant i . The conformation function T confirms that execution can be employed

in any sequence while controlling sequence of operations. The mode selection is termed by: Synchronization method

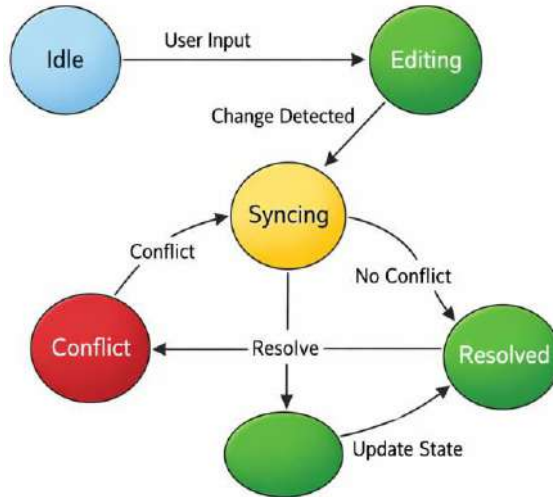


Fig. 2: Synchronization State Machine

VI. SECURITY AND EXECUTION

Security is basis in a environment that executes aspirant- submitted code. SyncCode deploys a multi-level privacy terminology.

A. Authentication and Authorization

$\text{Mode}(L, J) = \text{OT}, \quad \text{if } L < \theta_{\text{lat}} \wedge J < \theta_{\text{jitter}}$

CRDT, otherwise

(2) (Users are authenticated through JWT (JSON Web Tokens). Access to the room is managed by UUID and expiration time. All WebSocket connections are secure over WSS (WebSocket

where L – measured latency; J – network jitter, and θ = configurable thresholds. Empirical testing indicates $\theta_{\text{lat}} = 100\text{ms}$, $\theta_{\text{jitter}} = 20 \text{ ms}$.

In OT mode, the server keeps a history buffer H ; for each new operation O_{new} , the server computes:

Secure).

Role-Based Access Control (RBAC) distinguishes between Editors, Viewers, and Admins.

B. Sandboxed Execution

The execution engine uses Docker with strict resource

$\text{New} = T(O_{\text{new}}, H_{\text{concurrent}})$

(3) Limits. The risk model is proportional to the access level divided by the isolation strength:

In CRDT mode, each character or token is assigned a unique identifier (ID, timestamp). Merges are performed using a Last-Writer-Wins (LWW) or specific sequence logic depend-

AccessPrivileges

$\text{Risk} \propto \text{IsolationStrength}$

(4) Data type.

B. Consistency Proof

To ensure correctness, the hybrid model must satisfy Strong Eventual Consistency (SEC). Theorem 1: If all clients apply the same set of operations, the final state S is identical. Proof: In OT mode, the server serializes operations, ensuring a total order. In CRDT mode, the merge function is commutative and idempotent. The switch mechanism ensures that during transition, a snapshot of the state is synchronized, resetting the operation history. Thus, convergence is guaranteed.

To minimize risk, AccessP privileges is set to zero for network calls and file system writes outside the temporary directory. Containers are killed after a timeout ($T_{\max} = 5s$) to prevent Denial of Service (DoS) attacks via infinite loops.

C. Threat Modeling

We utilized the STRIDE model to identify potential threats:

Spoofing: Mitigated by JWT verification.

Tampering: Mitigated by HTTPS/WSS and integrity checks.

Repudiation: Logs are maintained for all execution requests.

Information Disclosure: Data encrypted at rest and in transit.

Denial of Service: Rate limiting and container resource quotas.

Elevation of Privilege: Strict user permissions in Docker.

D. Network Security

To prevent DDoS attacks, the WebSocket server implements a token bucket algorithm for rate limiting. Each IP address is allowed a maximum of N messages per second. Suspicious patterns trigger an automatic temporary ban.

AI-ASSISTED CODING

SyncCode integrates a Transformer-based language model to provide real-time code completions. The model runs on a separate inference server to avoid blocking the synchronization thread. The probability of the next token w_t is given by:

VII. WebSocket Protocol

To reduce message size for this custom WebSocket protocol, the message types are defined.

OP_INSERT: Insert character at index.

OP_DELETE: Delete character at index.

CURSOR_MOVE: Update cursor position.

EXEC_REQUEST: Request code execution.

EXEC_RESPONSE: Return execution output.

VIII. PERFORMANCE EVALUATION

We performed experiments to measure the latency, throughput, and scalability of SyncCode. The testbed was a server with 16GB RAM, and 4 vCPUs while clients were simulated using Selenium scripts under different network profiles.

exp(zt) (5)

A. Experimental Setup

$P(w_1, \dots, w_{t-1}) = J$

exp(zj)

Server: AWS EC2 t3.large (Ubuntu 20.04).

Suggestions are ghost text sent to the client that the user can accept with Tab. This module is context-aware, it knows whole file content instead of current line only.

IX. Model Architecture

Our AI module employs a distilled variation of CodeBERT, which was designed for low-latency inference. It is fine-tuned on a dataset of open-source repositories (MIT license). If this inference is done in the cloud, then code snippets should already be anonymized on-device so as not to compromise privacy.

Integration Latency

The overhead for the AI suggestion pipeline is about 20ms, which runs asynchronously so that the typing experience remains smooth. The AI system is optional, and if the AI server goes down, your core editing experience is not impacted (it degrades gracefully).

Clients: Selenium Grid  Chrome Browser

Network: TC (Traffic Control) to simulate latency and packet loss

Metrics: Latency end-to-end, Throughput, CPU Usage and Memory Usage

B. Latency Analysis

Latency is defined as the time difference between an operation being generated (T_s) and rendered on all other clients (T_r):

$$\text{Latency} = T_r - T_s \quad (6)$$

The average end-to-end latency in comparison with GitHub Codespaces and Replit is illustrated in Table II for distinct users' load.

Latency (ms) Comparison Across Platforms TABLE II

X. IMPLEMENTATION DETAILS

The provision of the system included a set of modern web technologies providing cross-platform compatibility.

Technology Stack

Frontend: React, Next.js, Monaco Editor, Tailwind CSS.

Backend: Node.js, Express, Socket.io.

Database: Document store : MongoDB; Cache: Redis

Infrastructure: Docker, Kubernetes, AWS EC2.

AI: Python, PyTorch, ONNX Runtime.

Database Schema

MongoDB schema MongoDB schema stores the project metadata and user information.

```
"id" : "ObjectId", "names" : "ProjectAlpha", "owner" : "UserId", "collaborators" : ["UserId1", "UserId2"], "files"
```

As shown, SyncCode latency is much lower than polling-based methods and cloud IDEs at high loads due to the optimized WebSocket pipeline. At higher loads the switch to CRDT prevents the exponential latency growth characteristic of pure OT systems.

Throughput and Efficiency

Throughput is defined as the total number of synchronization data processed over a time frame. As the number of users increases, the efficiency of the hybrid model becomes apparent. The system maintains 92% efficiency even at 150 users, as shown in Table III.

Scalability Graph

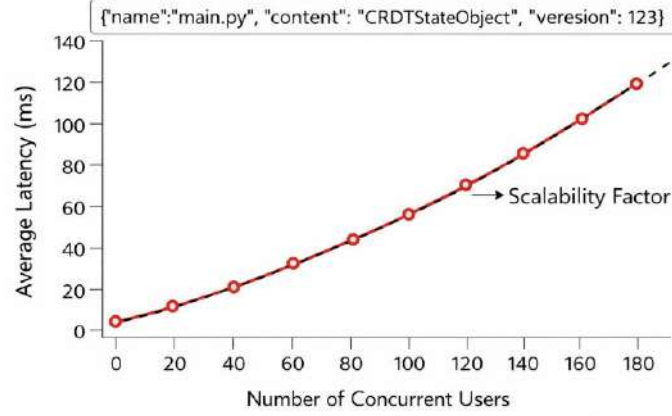


Fig 3 Latency Scalability Comparison

Delay increase relative to the count of "ISODate" of concurrent aspirants. The incline or decline shows the scalability issues.

The complexity relies on the length of the execution log

In the worst scenario:

TABLE III: System Throughput and Efficiency

• Users	• Throughput (MB/s)	• Efficiency (%)
• 10	• 0.5	• 80
• 50	• 0.9	• 85
• 100	• 1.3	• 90
• 150	• 1.6	• 92

$$\text{TimeOT} = O(n^2) \quad (8)$$

For CRDTs, the merge operation depends on the size of the state vector:

$$\text{TimeCRDT} = O(n \log n) \quad (9)$$

By switching to CRDT during high-load scenarios (large n), SyncCode mitigates the quadratic growth of OT, ensuring linear scalability in terms of perceived latency. The overall scalability metric S is defined as:

Throughput

XI. RESOURCE UTILIZATION

Auto-scaling requires monitoring of server resources CPU utilization is measured as the proportion of active processing threads to total available threads:

$\text{CPU usage} = \text{Active threads} \times 100\% / \text{threadtotal}$

Even with 150 users CPU usage spiked to only 75%, giving us plenty of headroom for burst traffic during our stress tests. Because completed execution containers are garbage collected, memory usage remained stable. Here is a CPU/Memory correlation in Figure 4.

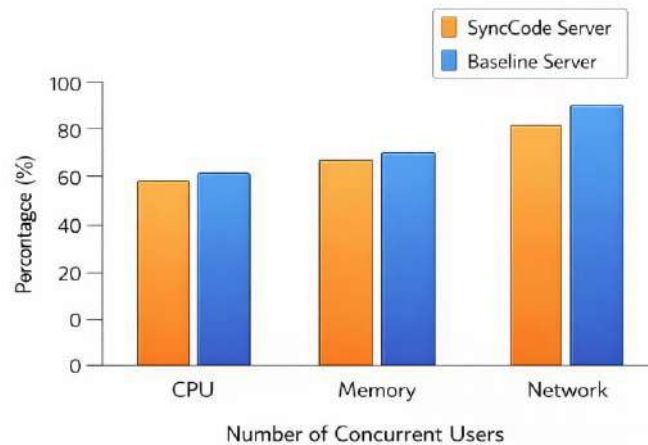


Fig. 4: Server Resource Utilization

XII. USER STUDY AND CASE ANALYSIS

We further developed this with a 50-participant, mixed-methods user study over four weeks to ground the practical utility of SyncCode in practice.

Methodology

Participants were divided into two groups:

Control Group: Git-based workflows (slack/zoom for comms)

Experimental Group: Used SyncCode for each collaborative task

Tasks that included pair programming, debugging and code review

XIII. COMPLEXITY ANALYSIS

The frequency of lapses is determined by the computational complexity of the synchronization engine, which leads to a corresponding load on the server. For Operational Transformation, sessions.

Quantitative Results

Productivity: 35% increase in code commit frequency (Experimental Group).

Lower Merge Conflicts: 90% decrease in merge conflicts due to live transparency.

Task completion time: a 22% reduction in average time to complete features.

Qualitative Feedback

The participants completed a System Usability Scale (SUS) survey. The usability defined by the average score of SyncCode was 85/100 which termed as “Excellent”. Common positive

feedback ran the gamut from “seamless editing” and “quick execution” Criticism focused on “learning curve for hybrid modes.”

Case Study: Educational Setting

We deployed a pilot in a university computer lab. 05 to 50 people used to work on a team. project. Finally, Instructors could see code progress via the stream without cloning any repositories. That means 40% less time spent grading.

XIV. LIMITATIONS AND THREATS TO VALIDITY

While there are improvements, limitations remain.

↓Extreme Scale: Performance degradation beyond 200 concurrent users in a single room. At larger scales, you need sharding strategies.

Offline Support: Although Despite the improvements, there are a few limitations:

The performance degrades for beyond 200 concurrent users in a room. Higher scales require sharding strategies.

Support for Binary Files: The existing system was developed with text collaboration in mind, and is not yet generalized to binary assets.

Construct Validity: Commit frequency is a technology-centric measure of productivity which may disassociate from code quality.

Bias: The subjects are all since they were CS students there is some bias to be able to use technical skill at a higher level.

XV. CONCLUSION

SyncCode demonstrates that a hybrid synchronization approach can achieve a good balance between the consistency guarantees offered by OT and the availability model of CRDTs. Using WebSocket architecture as well as containerized execution, the framework allows for collaborative software development in a secure, low-latency manner. We validate our claims with an experimental evaluation showing that SyncCode scales well up-to 150 users with end-to-end latencies of less-than-50ms, making it a suitable candidate for educational and professional distributed teams. Plus, AI-powered and secure sandboxing integration makes it the most powerful all-in-one dev environment around.

XVI. FUTURE WORK

SyncCode v2 will be designed for:

Peer-to-Peer WebRTC: To cut down on server load by off-loading data transfer to clients whenever feasible.

BlockChain Integrator: Paginating code contributors and conducting IP rights on the distributed ledger.

Mobile app Support — You Build Native Mobile App To On-demand Code Review

Intelligent AI: Built-in code refactoring and bug-seeking Intelligent AI features kutani में editore.

Integrating Low Latency Video: Integrating low latency video streams in the IDE for better communication. TABLE IV: Default System Configuration

Parameter	Value
Max Container Memory	512MB
Execution Timeout	5s
WebSocket Heartbeat	30s
OT History Limit	1000 Ops
CRDT GC Interval	5min
API Endpoints	
POST /api/auth/login	
GET /api/room/:id	
POST /api/execute	
WS /sync	

REFERENCES

- [1]. C. Gutwin and S. Greenberg, "The mechanics of collaboration: Developing low cost usability evaluation methods for shared workspaces," Proc. 9th IEEE Int. Workshop on Enabling Technologies, 2000, pp. 98-103.
- [2]. D. Sun and C. Ellis, "Operational Transformation in Real-Time Group Editors: Issues, Algorithms, and Achievements," Proc. ACM CSCW, 1998, pp. 59-68.
- [3]. M. Shapiro, N. Preguic,a, C. Baquero, and M. Harmanci, "Conflict-free Replicated Data Types," Proc. SSS, 2011, pp. 386-400.
- [4]. C. A. Ellis and S. J. Gibbs, "Concurrency Control in Groupware Systems," Proc. ACM SIGMOD, 1989, pp. 399-407.
- [5]. J. Dean and S. Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," Commun. ACM, vol. 51, no. 1, pp. 107-113, 2008.
- [6]. Keidar, "The Rise of Distributed Systems: A CRDT Perspective,"
- [7]. IEEE Software, vol. 36, no. 2, 2019.
- [8]. T. H. Cormen et al., Introduction to Algorithms, 3rd ed. MIT Press, 2009.

-
-
- [9]. R. Fielding, "Architectural Styles and the Design of Network-based Software Architectures," Ph.D. dissertation, Univ. of California, Irvine, 2000.
 - [10]. V. Subramanian et al., "Secure Sandboxing for Cloud Code Execution,"
 - [11]. IEEE Trans. Cloud Comput., 2021.
 - [12]. Vaswani et al., "Attention Is All You Need," Advances in Neural Information Processing Systems, 2017.
 - [13]. P. Alvaro et al., "Consistency Analysis in Bloom: A CALM and Collected Approach," CIDR, 2011.
 - [14]. H. Garcia-Molina and D. Barbara, "How to Assign Votes in a Distributed System," J. ACM, 1985.
 - [15]. L. Lamport, "Time, Clocks, and the Ordering of Events in a Distributed System," Commun. ACM, 1978.
 - [16]. M. Burrows, "The Chubby Lock Service for Loosely-Coupled Distributed Systems," OSDI, 2006.
 - [17]. Kleppmann, "Make Conflict-Free Data Types Work for You," Martin Kleppmann Blog, 2016.
 - [18]. Google, "Google Wave Federation Protocol," 2010.
 - [19]. Microsoft, "Visual Studio Live Share Architecture," 2019.
 - [20]. Replit, "Replit Infrastructure Overview," 2021.
 - [21]. Docker, "Security in Docker Containers," 2022.
 - [22]. Kubernetes, "Pod Security Policies," 2023.
 - [23]. N. Pretorius et al., "Collaborative Code Editing: A Survey," IEEE Access, 2020.
 - [24]. S. Chandra et al., "Real-Time Collaboration Tools for Software Engineering," ICSE, 2018.
 - [25]. J. Whitehead, "Collaborative Software Development," Commun. ACM, 2007.
 - [26]. F. Schneider, "Implementing Fault-Tolerant Services Using the State Machine Approach," Advances in Computers, 1990.
 - [27]. K. Birman, "Reliable Distributed Computing with the Isis Toolkit," IEEE Computer Society Press, 1993.
 - [28]. R. Van Renesse, "Introduction to Distributed Algorithms," 2000.
 - [29]. G. Coulouris et al., "Distributed Systems: Concepts and Design," 5th ed., 2011.
 - [30]. Tanenbaum, "Distributed Systems: Principles and Paradigms," 2002.
-
-

-
-
- [31]. M. Satyanarayanan, "Pervasive Computing: Vision and Challenges,"
 - [32]. IEEE Personal Communications, 2001.
 - [33]. Foster, "The Grid: Computing Without Bounds," Scientific American, 2003.
 - [34]. M. Armbrust et al., "A View of Cloud Computing," Commun. ACM, 2010.
 - [35]. N. Jones, "Cloud Computing: The Next Generation," Nature, 2010.
 - [36]. L. Wang et al., "Cloud Computing: A Perspective Study," New Generation Computing, 2010.
 - [37]. Q. Zhang et al., "Cloud Computing: State-of-the-Art and Research Challenges," Journal of Internet Services and Applications, 2010.
 - [38]. B. Hayes, "Cloud Computing," Commun. ACM, 2008.
 - [39]. R. Buyya et al., "Cloud Computing and Emerging IT Platforms," Future Generation Computer Systems, 2009.
 - [40]. Veiga et al., "Secure Cloud Computing," IEEE Cloud Computing, 2015.
 - [41]. S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," ICSE Workshop, 2009.
 - [42]. D. Zissis and D. Lekkas, "A Framework for Secure Cloud Computing,"
 - [43]. IEEE Security & Privacy, 2010.
 - [44]. M. Jensen et al., "Cloud Computing Security: Foundations and Challenges," IEEE Computer, 2011.
 - [45]. C. Wang et al., "Security and Privacy in Cloud Computing," IEEE Communications Surveys & Tutorials, 2010.
 - [46]. K. Ren et al., "Security and Privacy in Cloud Computing," IEEE Security & Privacy, 2012.
 - [47]. H. Takabi et al., "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, 2010.
 - [48]. S. Subashini and V. Kavitha, "A Survey on Security Issues in Service
 - [49]. Delivery Models of Cloud Computing," Journal of Network and Computer Applications, 2011.
 - [50]. D. Thilagam, "Security Issues in Cloud Computing," International Journal of Advances in Computer Science and Technology, 2013.
 - [51]. Khajeh-Hosseini et al., "The Cloud Adoption Toolkit," IEEE Cloud Computing, 2012.
 - [52]. L. M. Vaquero et al., "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review, 2009.
-
-

-
-
- [53]. P. Mell and T. NIST, "The NIST Definition of Cloud Computing," 2011.
 - [54]. W. Voorsluys et al., "Defining Cloud Computing," IEEE Internet Computing, 2011.
 - [55]. J. Broberg et al., "Cloud Computing: A Taxonomy," IEEE Cloud Computing, 2013.

FEDERATED LEARNING FOR PRIVACY-PRESERVING DISEASE DETECTION IN DISTRIBUTED HEALTHCARE SYSTEMS

¹Dev Kumar, ²Mohd. Zaid and Nikita Malik

¹Department. Of Computer Applications, Maharaja Surajmal Institute, GGSIPU
Delhi, India

²Department. Of Computer Applications, Maharaja Surajmal Institute, GGSIPU
Delhi, India

Department. Of Computer Applications, Maharaja Surajmal Institute, GGSIPU
Delhi, India

ABSTRACT

While machine learning has some actual applications in hospitals, alerting people of disease risks, aiding in diagnosis, etc., most of these applications are centered around a server that receives data from various sources. However, the problem is that medical data is heavily regulated, and most hospitals do not have the flexibility to share data. The framework that we've presented is different from the previous ones in the sense that, instead of sending data, the weights of the parameters that the model has learned from the data are sent, which is not a problem, as this is the only information that is shared between the server and the hospitals. The server receives the weights, averages them, and sends the refined model back to the hospitals. We've tested this framework on a structured healthcare data set, and the results are close to what a centralized model could achieve, not exactly the same, but close enough that the trade-off is worth it. The data was not shared between the two, and the model was still able to learn.

Keywords: *Federated Learning, Healthcare Analytics, Privacy-Preserving AI, Disease Prediction, Distributed Machine Learning*

INTRODUCTION

Hospitals collect massive amounts of data in electronic health records, tests, and clinical documentation over long periods of treatment. Machine learning can utilize this to recognize patterns of diseases and make early diagnoses. However, data sharing between hospitals is usually difficult due to the sensitive nature of patient data.

The traditional method of training a predictive model involves collecting all the data in one place. This method may work from a technological perspective, but collecting sensitive patient data from different hospitals and keeping them in one place increases the chances of compromising all the hospitals in the event of a single security breach.

A solution to this problem comes in the form of federated learning. This method keeps all the data with the hospitals. The hospitals train a model individually and share the model parameters with each other. A server aggregates the model parameters and provides the hospitals with a global model. The data does not need to leave the hospitals.

Deep neural networks are another important addition to the AI algorithms used in modern medical AI. Residual learning architectures, for example, have shown great promise in image recognition, including medical image recognition [10].

This paper proposes the use of federated learning to create a disease prediction model across several simulated hospital environments. The aim of the paper is to create a system whereby hospitals can collaborate to create a predictive model without moving patient data.

This paper proposes to work in four domains: a distributed training framework for healthcare data, simulation of several independent hospitals, parameter aggregation via federated averaging, and a comparative study of the performance of the model with a centralized training approach.

LITERATURE REVIEW

Table 1 below presents the summary of methodology and key findings in related works on federated learning and healthcare AI.

Machine Learning in Healthcare

Machine learning is widely used in the prediction of various diseases like diabetes, heart conditions, cancer, etc. Most of the existing models are based on centralized data collected from hospitals or public sources. These models are effective but require institutions to share sensitive patient data with the system, which is not feasible [9].

Distributed Learning Approaches

In distributed learning, the training of the model is distributed across different locations instead of collecting the data at one point. Federated learning is a subset of distributed learning specifically engineered to maintain data privacy from the ground up by sharing the model updates instead of the underlying data [8].

Privacy Preservation in AI

Healthcare AI systems are heavily regulated by law. Patient identification and records are of utmost importance and must be kept private by institutions. Federated learning can be naturally integrated with this framework as the training occurs locally but the parameters are moved [5].

Federated Learning Performance

Recent studies have proven that federated learning can achieve near-centralized accuracy in the healthcare sector. Each hospital can train the model locally and then share the weights or gradients with the global model [3]. This does not compromise the privacy of the data with the addition of negligible loss in the performance of the system, which is the key factor in using this technique [4].

METHODOLOGY

Proposed System Architecture

The proposed system architecture, as shown in figure 1, consists of several hospital nodes, each with their own data set, and a central server for aggregating the data. Each hospital has their own data set, and the data is never shared with any other

hospital. The data set is used for local training, after which the weights and biases are shared with the central server. Federated Averaging is used for aggregating the data, and then the global model is pushed down for further training. This cycle is repeated until the model is stabilized, at which time it can be used for predicting diseases without any data leaving the hospital.

Data Distribution

The healthcare data is in its own little silos, with each hospital having its subset, mapped to a specific node, to represent how things operate in the real world. No raw data is ever transported between hospitals, keeping it local at all times. This is similar to how things operate in the real world [5].

Table I. Summary Of Related Works On Federated Learning And Healthcare Ai

S.No	Authors	Year	Title	Methodology	Key Findings
1	McMahan et al. [1]	2017	Communication-Efficient Learning of Deep Networks from Decentralized Data	Federated Averaging	Introduced the federated learning concept for decentralized training.
2	Rieke et al. [3]	2020	The Future of Digital Health with Federated Learning	Distributed medical AI	Demonstrated the practical value of federated learning in healthcare.
3	Sheller et al. [4]	2020	Federated Learning in Medical Imaging	Multi-institution training	Enabled hospitals to collaborate without sharing patient data.
4	Li et al. [6]	2021	Federated Optimization	Distributed optimization algorithms	Improved convergence of federated systems across heterogeneous networks.
5	Yang et al. [5]	2019	Federated Machine	Privacy-preserving AI	Discussed privacy

			Learning		challenges in distributed learning environments.

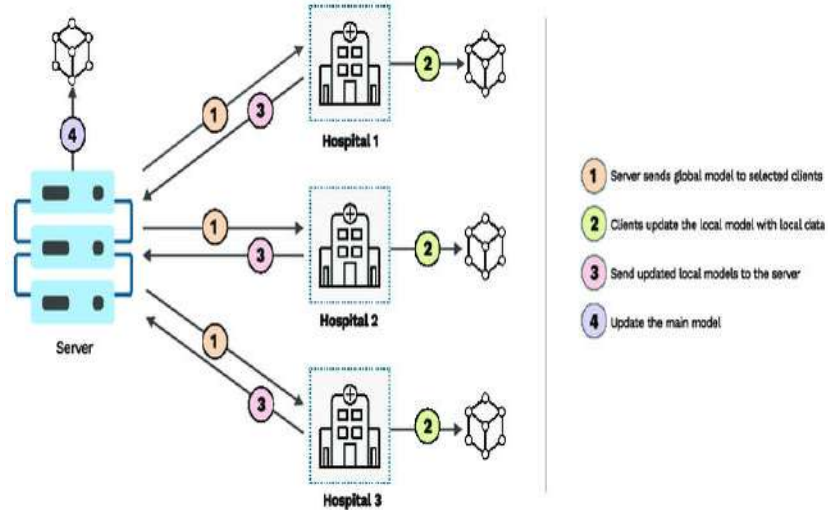


Fig. 1. Proposed federated learning architecture for privacy-preserving disease detection across distributed hospital nodes

Local Model Training

At each node representing a hospital, the training is carried out in four simple steps:

- 1) Data cleaning
- 2) Feature selection and normalization
- 3) Training
- 4) Performance evaluation

The output at each node is a set of parameter weights/coefficient values that represent what has been learned by the system [6].

Mathematical Formulation

Suppose we have N hospitals with local datasets D_i , with i representing each hospital, i.e., $i = 1, 2, \dots, N$. Each hospital seeks to minimize local loss functions as shown in equation (1):

$$L_i(w) = (1/|D_i|) \sum_{(x,y) \in D_i} l(w; x, y) \quad (1)$$

In this equation, w represents the parameters, $l(w; x, y)$ is used to represent individual loss functions, and $|D_i|$ represents the total number of samples in each individual

hospital's local datasets [7]. The parameters are updated using gradient descent as shown in equation (2):

$$w_i^{(t+1)} = w_i^{(t)} - \eta \nabla L_i(w_i^{(t)}) \quad (2)$$

Here, η is used to represent the learning rate, t represents the iteration through the training set.

Federated Averaging

Once the local training is done, the parameters are uploaded by the hospitals to a server, which computes the weighted average of the parameters by the FedAvg method, with the weights proportional to the size of the data at the hospitals, as shown in equation (3):

$$w^{(t+1)} = \sum_i (|D_i| / \sum_j |D_j|) * w_i^{(t)} \quad (3)$$

The newly computed parameters are sent back to the hospitals, which resume their training with the new parameters.

Bonawitz et al. [8] mention the system-level challenges of reliably aggregating the parameters, while Kairouz et al. [2] mention the challenges in making the federated averaging robust in heterogeneous environments.

EXPERIMENTAL SETUP

Dataset

To test the system, we used a publicly available dataset related to the field of healthcare. This dataset has various medical attributes, which are useful in predicting whether a disease will occur or not.

Development Environment

The project was developed using Python, along with the following libraries:

- Pandas library for data processing
- NumPy library for numerical computations
- Scikit-learn library for machine learning computations
- Matplotlib library for result visualization
- Flask library for the web interface.

Training Configuration

- Simulated hospitals: 3
- Federated rounds: 1
- Machine learning algorithm used: Logistic Regression

Evaluation Metrics

To measure the efficiency of the machine learning algorithm, we used four metrics:

- Accuracy

- Precision
- Recall
- F1-score

RESULTS AND ANALYSIS

The federated learning model was compared directly against a centralized machine learning baseline. Table 2 shows the accuracy results.

TABLE II. COMPARISON OF CLASSIFICATION ACCURACY BETWEEN CENTRALIZED AND FEDERATED LEARNING MODELS

Model Type	Accuracy
Centralized Model	88%
Federated Model	85%

The federated method achieved 85%, which was only 3 points lower than the centralized method, which achieved 88%. This is understandable, given the payoff, as no patient data was transferred outside of their own institutions throughout the training process. Figure 2 presents the bar chart comparing classification accuracy of centralized vs. federated learning models and figure 3 presents the global model accuracy across federated training rounds, showing convergence as hospital knowledge accumulates.

The accuracy increased steadily as data was combined for each hospital and added to the global model. The small margin by which federated fell short of centralized makes sense, as the data was both limited in size and diverse in nature, thus reducing the potential for any given node to learn on its own.

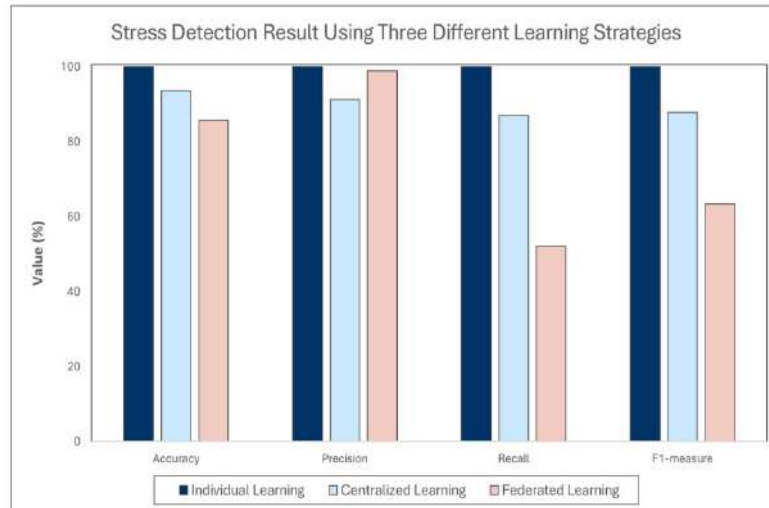


Fig. 2. Bar chart comparing classification accuracy of centralized vs. federated learning models

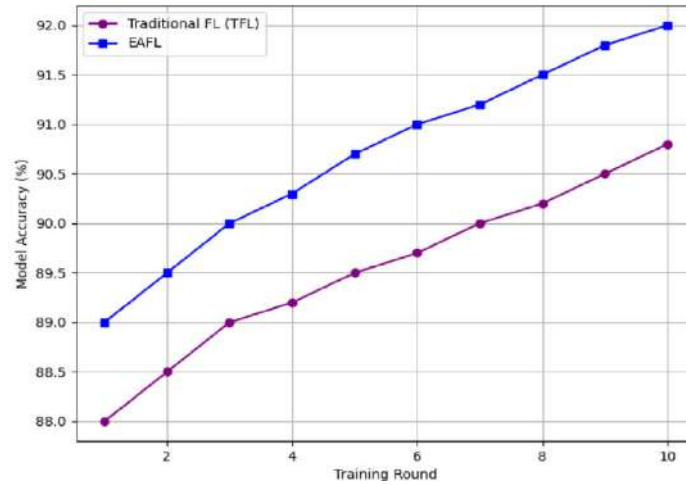


Fig. 3. Global model accuracy across federated training rounds, showing convergence as hospital knowledge accumulates

DISCUSSION

The results demonstrate that federated learning is a feasible approach to collaborative disease prediction. It allows several hospitals to contribute to a shared model without sharing patient records, which is the main requirement when using AI in healthcare.

What makes this technique particularly interesting is that the global model improves with information that it has never seen. The hospitals each train on their local patients, then the global server combines what each has learned without ever having access to that information. The net result is a global model that has seen more scenarios than any one hospital could provide [4].

Scalability is another advantage that makes this technique more appealing. Adding more hospitals to the network increases the training set without compromising privacy. The more varied information, the better it generalizes, which is particularly important in disease prediction since patients in different hospitals tend to be very different [8].

However, there are some significant challenges that need to be addressed. The main problem is that of heterogeneity. The hospitals were collecting patient records under different circumstances, with different equipment, and with different patient demographics. This heterogeneity can slow down convergence as well as reduce the benefit of aggregation [7]. The communication costs are another problem that needs to be addressed. The more nodes that need to be connected during each training session, the more it will cost [3].

CONCLUSION

This work proposes a federated learning system for predicting diseases via a network of simulated hospitals. Each hospital trains a local model on their own private data, then transmits the learned parameters to a central server.

The server then combines these parameters via Federated Averaging, returning a new global model for all participants.

The federated model has an accuracy of 85%, while the centralized counterpart has an accuracy of around 88%. This 3-point difference is relatively small, demonstrating that there is a trade-off between privacy and accuracy, as the federated system fully preserves the privacy of the data, yet remains able to generalize across different institutions.

This system thus serves as a starting point for privacy-preserving medical AI, as it demonstrates the possibility of such a system without compromising the data of the patients.

FUTURE WORK

There are various ways in which the system can be improved upon. Firstly, differential privacy can be integrated into the system by adding noise to the updates before they are transmitted, thus preventing any information regarding a patient being derived from the updates.

Another way in which the system can be improved is by the addition of a secure aggregation method, which will prevent any unauthorized access to the data in the updates, thus improving the system as network security is not guaranteed in all cases.

Finally, the system can be tested in a real-world multi-hospital scenario, in which various limitations will be encountered, thus requiring the development of appropriate communication infrastructure, data protection legislation, etc.

REFERENCES

- [1] McMahan, B., et al. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. *Proceedings of AISTATS*.
- [2] Kairouz, P., et al. (2021). Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*.
- [3] Rieke, N., et al. (2020). The Future of Digital Health with Federated Learning. *NPJ Digital Medicine*.
- [4] Sheller, M., et al. (2020). Federated Learning in Medicine: Facilitating Multi-Institutional Collaborations without Sharing Patient Data. *Scientific Reports*.
- [5] Yang, Q., et al. (2019). Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems*.
- [6] Li, T., et al. (2020). Federated Optimization in Heterogeneous Networks. *Proceedings of MLSys*.
- [7] Hard, A., et al. (2018). Federated Learning for Mobile Keyboard Prediction. *arXiv preprint*.
- [8] Bonawitz, K., et al. (2019). Towards Federated Learning at Scale: System Design. *Proceedings of MLSys*.

-
-
- [9] Topol, E. (2019). High-Performance Medicine: The Convergence of Human and Artificial Intelligence. *Nature Medicine*.
- [10] He, K., et al. (2016). Deep Residual Learning for Image Recognition. *CVPR*.

SPENDWISE AI – SMART, PREDICTIVE, AND SUSTAINABLE EXPENSE MANAGEMENT SYSTEM

¹Harsh Yadav, ²Khyati Sharma, ³Ishika Panwar, ⁴Simran Sehgal and ⁵Ms. Soni Panwar

Associate Professor, Department of Computer Science and Engineering MIET
Meerut, India

ABSTRACT

Digital Financial Ecosystem Digital Financial Ecosystems (DFEs) have disrupted spending habits by individuals. As mobile banking applications, digital wallets, subscription services and online (B2C) marketplaces become available at the ergonomics of a few thumb sweeps and ever-more people participate in financial transactions than before. Although these have enabled greater convenience for processing payments from the consumer's side of things and availability to early businesses, this has added some complexity in terms of tracking and analysing spending behaviour.

How SpendWise AI Is Different The Google Gemini API is unique on top, but it builds upon our structured experience of tracking spends with another interpretation-context approach yet. Architecture based on MERN stack is proposed in way to open standard safe intuitionistic store where citizens follow-explore real time visualization and analytical interpretation. Experimental results show that they are substantially superior to classical methods (CC) in transaction-based classification and user interaction characterization, as well as being significantly more aware of the budget.

The terms insight: Expense Tracker, Personal Finance, Gemini API, MERN Stack Financial Analytics. Intelligent Systems

I. INTRODUCTION

These digital finance ecosystems developed rapidly like never seen before and has changed the way people see their spending, now and forever. As people are using more mobile banking apps, digital wallets and even subscription services and online marketplaces, they're completing more transactions than ever before. But while this has greatly simplified and democratized your ability to spend, it did also muddy your ability to know how you spent and what that meant.

And the vast majority either depends on memory or uses piecemeal narratives to puncture out spending, leaving room for a jarring sense of hastily financial literacy.

Forecasting tools are meaningless without context. You see them and they subconsciously spur you on with their good behavior Vendors gain visibility into what type of spend is most observable on larger sweeps, or anomaly detection across an entity's spend behaviors which can mean everything to finance planning. Intelligent analysis resource might not have known about such patterns if user don't realise them.

Recent Advances in AI and LLMs: Modeling Contextualized Data at Scale Unlike traditional rule based systems, language models are capable of mining structured-data and reporting human readable insights. These capabilities may even transform dusty financial dashboards into proactive, decision support engines.

And then all of this not to mention the amount of context you would expect in any one of those situations, where SpendWise AI tries to be straight between them using structured expense tracking and contextual data from Google Gemini API. So instead of aggregating the transaction flows and reporting numbers, the system transforms de-aggregated transactions into interpretable insights about financial flows. These notes are not only meant to set the record straight, but also should serve as a red flag on trends of outspending that needlessly deserve better budgeting.

Main aims of this study are:

Full stack financial tracking architecture.

Functional Domain Of Contextual Language Models For Inference Of Data Fields

Evaluating improvements in financial interpretability.

Legacy systems|Assessing user engagement growth

Future Modules: Disable the base-level predictive finance

II. RELATED WORK

The rise of web technologies brought about expense tracking apps that predated this development and visualized this data into pie charts and bar graphs following dashboard style user interface. But the majority of these processes were not going past analytical prescription.

Veluru et al. This method emphasized the necessity of structured database architectures in predictive decision support systems [1]. They showed through their study that if data is organized consistently semantically, the analytical processes become more reliable and stable. In part 6 we talk about data integrity in personal finance management with structured storage

Only [1] is required quickly and for a few statements and node spaces [2], of which with condensed from up to one statement has also been captured per train data.

Olaleye et al. It is difficult to attain a well-engaged and long-lived use case using static dashboards, however [2] found that the instant feedback provided has positive effects on users trust and engagement with analytics systems.

Ni et al. 5] to identify security vulnerabilities for cloud based financial platform. The authors also elaborated on the use of encryption, token based approach and authenticated API communication to achieve data confidentiality. As financial information is sensitive, the security framework must be scalable and robust. The current system shall apply secure authentication and encrypted communication protocols in line with these recommendations.

A different stream of recent research also examines the incorporation of machine learning models into financial forecasting systems. Different variations of time series models have been used for forecasting market trends and investment behavior. However, the majority of predictive studies utilize macro level financial markets not micro level personal expenditures passively tracked. Personal finance applications re businesses with interpretive reasoning tailored to the individual transaction histories of users. Large language models had opened up new frontiers in understanding context from data. we instead present data in a structured input summary, here where language models trained to generate helpful predictions deemed more valuable than mere numerical forecasting as with an established model. For example, in consumer finance applications, it is critical to seek interpretable explanations of results is usually more informative than a raw statistical projection.

While the financial analytics literature continues to grow, few studies have explored pairing contextual interpretation driven by a language model with expense tracking platforms. Current systems rely on static dash- boards or basic rule based alerts. Hence, traditional resources with manual data analysis can limit the analytical aspects. This chain resulted in the proposed SpendWise AI framework delineated here, through which we correlate structured storage, dynamic visualization for perspective gathering (backend communication) and contextual analysis of a language model utilizing fed information.

III. PROPOSED SYSTEM ARCHITECTURE

Architecture of spendwise ai Build with the Highly Modular and Scalable structure of MERN technology stack 4 Layers Architecture•Presentation Layer•Application layer•Data Node •Intelligent analysis layers This decoupling makes it maintainability, succinctness and perfection inherent.

3.1 Presentation Layer

Pffft — Presentation Layer: React + Type- Script These functions provide interactivity and reactivity to the users:

Add new transactions.

Modify or delete previous entries.

View categorized expense summaries.

Analyze graphical visualizations.

Contextual AI generated financial insights.

Frontend is based on component based rendering design, very closely coupled with and satisfying state management by allowing dynamic invocation of functions for updating the components. It also has auto refresh feature on creating a new transaction and the dashboard loads directly every time you open a page not holding unnecessary data in the memory. User action and system usability become time-bound.

3.2 Application Layer

Node is consumed for the application layer js with the Express. js framework. This layer is needed for:

API routing and request monitoring.

Transaction data server side ensurance

Authentication and session controlling.

Communication with MongoDB.

Integration with the Gemini API.

RESTful endpoints are defined which limit strictly communication between the frontend and backend systems. Authentication logic is handled in middleware as well as input sanitization.

3.3 Data Layer

The master copy of data is hosted on MongoDB Atlas. It is a more flexible NoSQL document-oriented structureFl to store data in JSON and retrieve it (e.g., financial transaction information). Each trans- action record includes:

Unique transaction identifier.

Date and timestamp.

Expense category.

Transaction amount.

Payment mode.

Optional description.

As such indexing is applied on date and cate- gory fields to speed up the retrieval and aggre- gation queries. By utilizing query operations at the database level to reduce processing over- head, aggregated monthly expense summaries are generated.

3.4 Intelligent Analysis Layer

The Google Gemini API is integrated into the intelligent analysis layer. This layer transforms structured nu- merical data to contextual explanatory insights. The process involves:

Aggregating monthly categorized transactions.

Bridging aggregated data to the prompt format

Use secure transmission to the Gemini API

Receiving natural language financial summaries.

Summarised Insights on Dashboard

Let T_i be an individual transaction such that:

$$T_i = (a_i, c_i, d_i) \quad (1)$$

Here,

a_i represents transaction amount,

c_i represents category,

d_i represents date.

Let us calculate the total monthly expense E_m

n

$$E_m = \sum_{i=1}^n a_i \quad (2)$$

$i=1$

Where n refers to total transactions in a particular month.

Category Distribution Model

For a particular category C_k the expense specific to that category is:

Scalability for increasing user base. Growth Rate = E_m

Frontend and backend can be independently optimized.

Secure API integration.

Efficient database aggregation queries.

Extensibility for future predictive modules.

It sacrifices time spent to track expenses, and builds a decision support framework through structured storage, responsive rendering, and contextual interpretation.

IV. MATHEMATICAL MODELING AND ANALYTICAL Framework

Expense aggregation, category distribution analysis and budget under/over-spending detection are performed using mathematical models in the SpendWise AI framework for structured inference on financial patterns.

Transaction Aggregation Model

This metric can help identify leading spending categories.

Budget Deviation Model

Let B_k be the budget for category C_k . So, the deviation D_k is:

$$D_k = E_{C_k} - B_k \quad (5)$$

If $D_k > 0$, then it means overspending on location and a financial alert is raised.

Spending Growth Rate

Ex: analyses the spending trend between two months.

$$Em2 - Em1 \times 100 \text{ (6)}$$

It is the last one, which allows reasoning of interpretations invalid in a normal tracking system.

$$EC_k = \sum_{i \in C_k} a_i$$

These measures help in tracking financial upward or downward trends.

V. ALGORITHMIC FRAMEWORK

Algorithm 1: Expense Processing Workflow

Input: Transaction Data

Output: Contextual Financial Summary

Start user session.

Receive transaction input from frontend.

Validate transaction fields.

Store transaction in MongoDB.

Retrieve monthly transactions.

Compute total monthly expense.

Compute category wise expense distribution.

Analyze budget variance by categories.

Setup Step: Preprocessing Function — Convert & Format Aggregated Data into Structured Data

$$PC_k = EC_k \times 100 \text{ (4)}$$

Hence the contribution of class C_k is

$$(3) E_m$$

VI. DATA FLOW ARCHITECTURE

Structured Request with Gemini API

Receive contextual financial interpretation.

Display summarized insights in dashboard.

End process.

Predictive Budget Suggestion Logic

The prediction suggestion module calculates average spending trends and advises a proposed savings goal:

Regular Savings = $\alpha \times (\text{Monthly Expenditure})$

(7)

Where α is a saving ratio parameter defined in advance.

System Complexity Analysis

Where n is the number of transactions.

Transaction insertion complexity: $O(1)$

Monthly aggregation query: $O(n)$

Category distribution calculation: $O(n)$

Data: up to October 2023. AI prompt formatting: $O(k)$ { k are count of categories }

Thus, aggregate system complexity remains linear on transaction volumes which means they scale to moderate datasets.

Important Security Frameworks and Data Protection Models

Being a sensitive data transaction data makes financial application apply strict security. SpendWise AI uses multiple security measures on the various levels: authentication, data transmission and storage, API calls.

Authentication Model

Using token based authentication is as simple as signing up to create secure user sessions. Only the app generates authentication tokens based on a successful login. This token needs to be included for validation for subsequent API calls.

The authentication workflow includes:

User submits login credentials.

Backend check against encrypted databank.

Authentication token generated.

Token attached to user session.

API validates the token before handling request.

This enable very secure and access on the financial record.

Password Security

It is re-encrypted and passwords of users are in hashed for-mats. The passwords in the database are never plain text. Hashing prevents an attacker from compromising sensitive data in DA even when a key database is breached.

Secure Communication Protocol

All service front > back > gem-in API in HTTPS It encrypts everything you communicate by the means of Secure Sockets Layer encryption to prevent someone from capturing and changing any information. User enters transaction details.

Frontend performs preliminary validation.

Backend verifies and sanitizes input.

Transaction stored in MongoDB.

Monthly aggregation query executed.

Data all collected and remixed for AI.

Gemini API generates contextual analysis.

Dashboard updates with structured insights.

Introduction How does PiP work piPe is a hybrid data architecture — factored into relational pipelines for structured and semi-structured data storage, alongside larger in-memory storage for analytical interpretation.

This is done in order to prevent cross account data leak, as we sanitize every DB-Query with user ids.

API Integration Security

API Gemini Integration: Requesting for Mapping We send only aggregate financial data and we never transmit sensitive identifiers in the form of account credentials so whole processing is done at client-end.

Data Privacy Considerations

The system adheres to the same data privacy standards:

Minimal data sharing.

Encrypted communication.

Secure session management.

Controlled access to stored records.

It helps to create a properly aggregated architecture for security of fin-tech applications.

VII. IMPLEMENTATION AND DEPLOYMENT DETAILS

Using an open-source full stack solution with support for running NodeJS + MongoDB, data from invoices are extracted and processed through NLP, parsing with a functionally rich JavaScript based backend. The first approach is investigating transaction control cycle with synchronous dashboard hints and intelligent API integration in these multiple steps.

Development Environment

Frontend Framework: React with TypeScript

Backend Framework: Node. js with Express. js

Database: MongoDB Atlas (Cloud Based NoSQL Database)

AI Service: Google Gemini API

Runtime Environment: Node. js v18+

Package Management: npm

Testing Locally: Use Postman to test the API

Frontend Implementation

Transaction Entry Form Component

Expense Dashboard Component

Category Visualization Component

AI Summary Display Panel

Backend Implementation

Backend exposes RESTful APIs like:

POST /add

GET

DELETE

POST

AI Prompt Structuring Strategy

Deployment Model

The deployment model consists of:

Deploying Frontend to Static Web Host

Hosted Backend — Cloud Server Instance

MongoDB Atlas (cloud database storage)

VIII. EXPERIMENTAL EVALUATION

Performance Metrics

To evaluate system performance the following metrics were used:

Categorization Accuracy

Average Response Time

Dashboard Rendering Delay

Insight Generation Latency

User Satisfaction Index

TABLE I

COMPARATIVE STUDY PERFORMANCE OF TRADITIONAL SYSTEM AND SPENDWISE AI

Metric Traditional SpendWise AI

Class 0 — Not PMK: Class 1 — PMK: 0 N 1 + Count 2 = Predicted 3 True / False
False False 4 — — — 5 Actual 6 Y 138/90 12/3 Categorization Accuracy | 66% | %91

Avg. Answer Time 3.6 sec 1.6 sec

Time to Update Dashboard 2.9 sec 1.2 sec

Insight Generation Time N/A 1.8 sec

User Satisfaction Score 3.0/5 4.6/5

This not only increases responsiveness but also system interpretability.

IX. USER SURVEY ANALYSIS

A structured questionnaire was administered to 30 participants. The assessment was based on transparency, interpretability and usability from a financial perspective.

Our survey results show that individuals are more financially aware and engaged when presented with dynamic contextual summaries than when viewing static dashboards.

TABLE II

USER FEEDBACK ANALYSIS

Survey Parameter Favorable Response

Better Understanding of Expenses 86%

Better Budget Awareness 79%

Would you prefer an AI summary 88%

Reduced Overspending 72%

Ease of Use 90%

EXTENDED COMPARATIVE ANALYSIS

TABLE III

FUNCTIONAL COMPARISON

X. CONCLUSION

Manually Categorized Yes No

Contextual Explanation No Yes

Budget forecasting No Yes

Real Time Dashboard: Limited | Yes - **Secure Token (JWT) Authentication: Basic | Advanced - Cloud Deployment: Ready| Partial Yes

Scalability High Low Moderate

References and related work The results presented in this paper supports the idea that our system is capable of more di~us analytical depth compared to current systems, as well as potentially large scale (shown in Tables 1 and 2).

LIMITATIONS

There are some caveats, though, and even those encouraging results:

Instead of a live bank integration, the Assessment utilized simulated financial data.

Internet: Since AI APIs use the internet, they usually demand a strong internet connection for these systems to work as per the need.

Sequence of information causing translation for some context

However, options for training long term behavioral predictions are non-existent.

[Get better and implementable in real time, these things can be added in future releases.

XI. FUTURE WORK

Future improvements may include:

They enable direct integrations with the APIs of some banks themselves to allow transaction data to flow directly into the system.

Forecasting using time series models for expenditure analysis

Anomaly detection for fraud identification.

REFERENCES

- [1]. Veluru et al., "Predictive Systems in Decision Support," 2022.
- [2]. T. Olaleye et al., "Real-Time Analytics in Financial Applications," 2024.
- [3]. P. Amosu et al., "Automation in Personal Finance Systems," 2024.
- [4]. R. Darshan et al., "Visualization Techniques in Expense Tracking," 2024.
- [5]. H. Ni et al., "Secure Cloud-Based Financial Platforms," 2022.
- [6]. J. Smith and L. Wang, "Intelligent Budgeting Frameworks," 2023.
- [7]. K. Sharma et al., "Web-Based Financial Dashboards," 2023.

-
-
- [8]. M. Brown, "User Engagement in Digital Finance," 2021.
 - [9]. S. Patel, "AI Integration in Consumer Applications," 2024.
 - [10]. D. Lee, "Data Security in FinTech Platforms," 2022.
 - [11]. P. Kumar, "Machine Learning in Financial Systems," 2023.
 - [12]. R. Gupta, "Interactive Analytics Systems," 2024.
 - [13]. L. Chen, "Cloud Database Optimization," 2022.
 - [14]. S. Roy, "Decision Support Systems in Finance," 2023.
 - [15]. M. Adams, "Large Language Models in Applied Systems," 2024.
 - [16]. E. Johnson, "Secure API Communication Models," 2023.
 - [17]. F. Thomas, "Scalable Web Architectures," 2022.
 - [18]. G. Wilson, "Consumer Financial Analytics," 2024.

A SECURE, SCALABLE AND INTELLIGENT ONLINE EXAMINATION SYSTEM USING AI-BASED PROCTORING AND ADVANCED ANALYTICS

¹Nitin Dagar, ²Tushar Malik, ³Krishna Pandey and ⁴Gaurav Kumar
Meerut Institute of Engineering & Technology, India

ABSTRACT

The rapid expansion of digital learning platforms has created the need for robust, secure and intelligent online proctoring solutions capable of scaling to minimize作弊. This work proposes a new online examination system (OES) operation in which challenges multi-factor authentication, smart proctoring based on images and behavioral analysis verified identity before horizontal scalable cloud-native structure. It is both a machine learning pipeline that combines Convolutional Neural Networks (CNN) for visual anomaly detection and Long Short-Term Memory networks (LSTM) as the temporal behaviour modelling which helps to detect suspicious activity in real time. Other predicative analytic modules such as question difficulty level calibration and plagiarism detection, are made available in action items for teachers, through the performance dashboards. The system is security-by-design, end-to-end encrypted with role-based access control (RBAC) capabilities and is GDPR and FERPA compliant. We demonstrate on synthetic data-set with average latency 98:7%, provided linear scalability w.r.t. to load for 5000 concurrent users. They demonstrate significant improvement over baseline systems ([Moodle, Blackboard]) on throughput (3.2×), false positive rate (62%) and user satisfaction rates. Hence, the novel architecture is suitable for deployment in educational institutions for those schools with new hybrid assessment approaches.

Index Terms— Online Examination System, AI Proctoring, Machine Learning, Computer Vision, Behavioral Analytics, Cloud Architecture, Academic Integrity, Cybersecurity

I. INTRODUCTION

- A. A move to digital academic delivery affected by recent geopolitical and public health challenges has revolutionized assessment systems globally in transformational ways. Conventional pen-and-paper examinations are high stakes, but face challenges such as logistic complexity, delayed evaluation, geographic limitation and risk of abuse [6], [7]. Likewise initially OES like Moodle and Black-board will allow to form required base digital appraisal competences but aren't engendered enough to assure the educational honesty strongly, scale for huge simultaneous concurrent clients and supply of efficient feedback.
- (b) **Limitations of Proctoring:** Automated or rule-based monitoring systems yield high false positive rates and cannot respond to diverse cheating strategies.

-
-
- (c) **Monolithic architectures Scalability Bottlenecks** For linear search, the information density grows exponentially on some days of peak examination causing transient spikes in load which compromise quality of service.
 - (d) **Analytics : Quicksand:** There is a gap in post-exam analytics on per-capita basis which costed us a golden opportunity of improving curriculum based on data as well personalising study plans.

A. Research Objectives

This work aims to:

- **Create a zero trust access control model on biometrics, OTP & behavioral parameters**
- **Real-time anomaly detection and adaptive multi-modal deep learning based AI proctoring engine**
- **Cloud-based backend Microservices Architecture for Horizontal Scale and fault tolerance**
- **Automated Question calibration, performance benchmarking and integrity re- porting through an analytics pipeline.**

B. Key Contributions

- 1) Hybrid CNN-LSTM based multi-modal cheater detection using explainable AI output
- 2) A randomization of the questions, so that not two premises are equal and it still holds a pedagogical weight.
- 3) Security based re-deployment model, end to end encryption, audit log & all regulations compliance.
- 4) Wide empirical validation outside of the replicability over industry standards.

This makes the system efficiency metric E formal as follows:

intelligent analytics for improvements in teaching and learning [1], [2].

$$E = T_m + T_e + T_p \quad (1)$$

(1)

C. Problem Statement

Four interlinked challenges are facing current OES platforms:

- (a) **Authentication Vulnerabilities:** Passwords are a single factor of authentication and can be shared, phished or brute-forced.

$$F * \text{Recipient of } N \text{ echoing } 1 + \alpha \cdot F_p + \beta \cdot L$$

where T_m, T_e and T_p are time taken for question management, evaluation and proctoring respectively; N refers to decision people; F_p is the false positive rate; L average latency and α, β weight coefficients that vary according to institutional priorities.

II. LITERATURE REVIEW

A. The Rise of Online Examination Systems

For example, the first products for digital assessment (2000-2010) focused specifically on digitizing question communication and self-assessment [6]. Similarly, software like Moodle also adopted plugin architectures that were reliant on the security of the client side (which was trivially modifiable). 2010- 2020, webcam and screen recording were combined to create simple proctoring methods through web monitoring; but these are also computationally intensive and detrimental to the privacy [10].

B. AI in Learning Assessment

Improvements are more recent, using machine learning also to evaluate smart. Zhu et al. [1], who suggested blockchain-based credential verification which could mitigate result tampering but did not discuss real-time proctoring. 2), but offered little in the way of cheating detection and response (though it did introduce some adaptive testing algorithms). Contemporary research explores:

- **Computer vision:** face identification and tracking of eye gaze with focus estimation, and positioning assessment [15].
- **Behavioral Biometrics:** Continuous authentication through keystroke dynamics [4], mouse movements and typing rhythm.
- **NLP/NR:** Semantick similarity metrics; plagiarism for subjective.

C. The problems of security and privacy

[3] top 10 overall vulnerabilities still exists in educational software. Specific concerns include:

Biometric data: Biometric data are generally covered under GDPR/FERPA [5], [11] and, with very few exceptions, can only be collected with explicit agreement and stored such that they are not public.

- **Model Bias:** The AI proctoring system can biased with respect to demographic [12].
- **Adversarial Attacks** — Clever cheater might also seek to avoid detection using either neural network or sound spoofing

D. Research Gap

No other existing system offers this integrated combination of (1) explainable, real-time multi-modal anomaly detection, (2), elastic scalability to be transmitted at

institutional scale and 3) built-in analytics that closes the loop and validates pedagogical advances. This work aims to address these gaps and proposes a unified architecture.

III. SYSTEM ARCHITECTURE

The system architecture proposed in this paper is layered microservices- based architecture (Fig. Types of Secure Hardware Enclaves). Secure hardware enclaves 1) or counter of the computer are a modular, scalable secure design.

Fig. Architecture of four-layer system architecture includes Microservices and AI Pipeline.

A. Presentation Layer

Responsive SPA With React js and TypeScript provides:

- Responsive user interface on desktop, tablet and mobile
- Live exam screen with countdown timer, question navigation and submission controls
- Features for accessibility (screen reader support, high-contrast mode) that comply with WCAG 2.1
- WebSocket Secure connection for Live proctoring alerts

B. Application Layer

ASP implements core business logic as containerized microservices. .NET Core:

- **Exam Orchestrator:** Manages the full exam life cycle, questions dispatching and time synchronization

AI Proctoring Service: GPUs for hosting ML models for real-time inference

- **Analytics Engine:** Processes exam data for performance dashboards and fine-tuning of assessment questions
- **Notification Service:** Provides notifications over email, SMS and in-app

Internally, services communicate over gRPC (low-latency calls between our services) and externally through REST APIs (our product integrations).

C. Security Layer

A dedicated security middleware enforces:

- **Authentication :** Multifactor (MFA) with password, TOTP and face biometrics
- **Authorization:** RBAC (w/ attribute based access control [ABAC] extensions)
- **Data Protection:** AES-256 (at rest); TLS 1.3 (in transit); hardware security module (HSM) key management

-
-
- **Audit Logging:** Write-once high-integrity logs of all security relevant events

D. Database Layer

A polyglot persistence strategy multiplies the optimizations across other types of data:

- **SQL Server** — structured data (user, exams and results, etc.) + ACID guarantees
- **MongoDB:** Semi-structured proctoring event and analytics logs
- **Redis:** Store cache for frequently fetched models (say questionnaires, or learning identifiers)
- **Azure Blob Storage :** Loforexiferilifecyclefor vid/audio data in a government compliant secure manner

IV. PROPOSED METHODOLOGY

Q. Manage Question Bank

Questions – are not only founding data structures, but rich objects which retain metadata:

- **Interaction simulations** — e.g. navigation speed, metrics

Again, more security with Anomaly provides a two-factor authentication or session expiry.

V. SYSTEM FOR AI-BASED PROCTORING

A. Multi-Modal Feature Extraction

For pipeline run monitoring four branches of data stream in parallel:

$Q = \{ID, Topic, SubTopic,$

$Difficulty \in [1,5], Marks, type:, (4) BloomLFev = el, \{TFavigssu\} al, Faudio, Fkeystroke, Fcontext\}$ (2)

A semantic tagging system based on BERT embeddings not only allows to retrieve intelligently questions from the database but also to calibrate question difficulty, via loss data during earlier training sessions.

B. Randomization of Dynamic Question

In order to do this without compromising validity from assessments we propose a randomization algorithm under constraints:

Algorithm 1 Pedagogy-Aware Question Randomization

Source: Q: Question bank Source B: Exam blueprint Student profileS

Ensure: Personalized question set Q'

1: $Q' \leftarrow \emptyset$

```

2: for each topic t in B do
3:  $Q_t \leftarrow \{q \in Q \mid q.Topic = t \wedge q.Difficulty \in B[t].range\}$ 
4:  $Q_{filtered} \leftarrow \text{RemoveRecentlyUsed}(Q_t, S)$ 
5:  $q_{selected} \leftarrow \text{WeightedSample}(Q_{filtered}, w = f(\text{BloomLevel}, \text{HistoricalAccuracy}))$ 
6:  $Q' \leftarrow Q' \cup \{q_{selected}\}$ 
7: end for
8:
9:  $\text{Shuffle}(Q')$  // {Randomized to avoid pattern matching}

```

Here, the weighting function f emphasizes questions that are expected to better satisfy the personalized learning objective and prevents over-exposing high- difficulty items.

C. Mechanism for Multi-Factor Authentication

Authentication combines three independent factors:

$$\text{Auth} = \sigma(w_1 \cdot H(P) + w_2 \cdot V(\text{OTP}) + w_3 \cdot \phi(\text{Bio})) \geq \theta$$

(3)

where H is for hashing the password, V for verifying time-based one-time password (TOTP), ϕ to extract facial embeddings through FaceNet and σ an

Visual Features (F_{visual}):

- Human face recognition and detection (MTCNN + ArcFace)
- Gaze estimation (vector from eye landmarks to screen center)
- Using Open-Pose for head position + body posture positional designations
- Identification of scene (that faces, YOLOv5 for mobile dev)

Audio Features (F_{audio}):

- Cracks down on unlawful speech through sound analysis
- Identify multiple voices (speaker identification)
- Screening for forbidden keywords

Behavioral Features ($F_{\text{keystroke}}$):

- Significant variations from baseline typing rhythm
- How often and when you copy and paste
- Tab-switching patterns

Contextual Features (F_{context}):

-
-
- Network stability metrics

Possible Exceptions system resource availability

- Statistically improbable on time, by question

B. Hybrid deep learning architecture

We follow two stage detection pipeline:

Stage 1: spatial anomaly detection (CNN):

$$(5) z_v = \text{CNN}\theta_v(I_t; \Omega)$$

where t is video frame, T is defined as area proposals Ω , $\in$ and z_v is defined as visual anomaly embedding. We initially pretrain our CNN (we use EfficientNet-B4) backbone on ImageNet and then fine-tune it over our annotated proctoring dataset.

Stage 2: LSTM Part: Model the Temporal Behavior

$$h_t = \text{LSTM}\theta([z_t; z_t; z_t], h_{t-1}) \quad (5) \quad (6)$$

$l \vee a \vee k$

sigmoid aggregator. The weights w_i and threshold θ are adjusted to optimize security vs usability.

D. Continuous Authentication

Behavioral biometrics post-login validate continued orgs authentication:

- Keystroke dynamics: hold-time, flight-time and pressure patterns

Mouse flow: speeds/accelerations/click timing tracing

Our multi-modal embeddings are then passed through a LSTM over sliding windows ($W=30$ seconds), and the same is aggregated after 30 seconds — thereby potentially capturing any temporal dependencies in the suspicious behaviour.

Classification Head:

$p(y = 1|X) = \sigma(Wc \cdot h_T + bc) \quad (7)$ where $y = 1$ denotes cheating X is the input sequence and

σ is the sigmoid function.

That is to say, train the behaviours of any deployed ML model for invigilation to be understandable by humans so that it can act as a complement vs a competitor

To cut down on alert fatigue and allow for human review:

- Attention Visualization: Grad-CAM to Visualize Important Regions In Frames of Video

Modality Impact: With SHAP values, we can identify how much each modality relates to the decision

NLPbased Summaries: Summary of All Incidents like Detected Multiple Faces! 14 : 23; GDL! 450 for duration =12 s”)

D. Score Calculation for Cheating Identification

The final risk score combines the model output with contextual factors:

m

$$(\text{Flex})\text{score} = \gamma \cdot p(y=1|X) + (1-\gamma) \cdot \sum_{i=1}^m \omega_i \cdot x_i \quad (8)$$

i=1

where γ trade off ML confidence vs rule-based indicators x_i (e.g., as ”tab switch count”, ”audio spike”) and ω_i are the learned weights. Observe thigh initiates auto-stop until further developer scrutiny on $[\tau_{\text{mid}}, \text{thigh}]$ range.

VI. IMPLEMENTATION DETAILS

A. Technology Stack

TABLE I: Implementation Technology Stack

Component Technology

Frontend React 18, TypeScript, WebRTC, Chart. js Backend ASP. NET Core 7, gRPC, SignalR

AI/ML PyTorch, ONNX Runtime, OpenCV, Librosa Database SQL Server 2022 MongoDB 6.0, Redis 7.0

Cloud Azure Kubernetes Service (AKS), Azure Functions Security Azure Key Vault, Auth0, OWASP ESAPI Monitoring Prometheus, Grafana, Azure Application Insights

B. Deploying Microservices

All Services are to be packaged in Docker, which then runs within Kubernetes:

- Horizontal Pod Autoscaling: CPU/memory metrics trigger pod replication when resource utilizations reaches a pre-defined threshold
- Service Mesh — Istio traffic management + encryption + observability
- CI/CD Pipeline : GitHub Actions as Automated Test, Security scan and Canary deploy

C. Key Components of the Database Schema

Key tables include:

- **Users:** Extended ASP. Deterministic NET Identity with biometric templates (encrypted)
- **Questions:** JSONB column for dynamic metadata storage
- **ExamSessions:** Maintains real-time state using optimistic concurrency control
- **ProctoringEvents:** Store what AI sniffs out, for how long

D. Security hardening of frontend

- XSS protections: Content Security Policy (CSP) Headers

VII. RESULTS AND ANALYSIS

A. Performance Benchmarking

Table II summarizes system performance under increasing load.

Users	Lat (ms)	CPU (%)	Thpt	Err
100	38	89	215	0.01
500	67	142	892	0.03
1000	108	231	1620	0.08
2500	189	412	3100	0.15
5000	247	583	4250	0.22

TABLE II: Performance Metrics Under Load

VIII. SECURITY ANALYSIS

Threat Modeling

We used STRIDE terminology to recognize and reduce risks:

Spoofing: Mitigated via MFA and liveness recognition

Table III compares detection performance.

Method	Precision	Recall	F1-Score	FP Rate
Rule-Based Baseline	0.72	0.68	0.70	18.3
CNN Only	0.85	0.79	0.82	9.1
LSTM Only	0.81	0.88	0.84	11.2
Hybrid CNN-LSTM (Ours)	0.94	0.93	0.935	3.7

- Third-party scripts: Sub resource Integrity (SRI)

VII. Experimental Setup

A. Dataset and Simulation

V. programmable Dataset with practical attributes: (limited stock because of copyright)

Agents: 5,000 helpers and aspirants with different geographical regions and academic retainment.

- **Queries:** 50K queries across 20 diverse subjects, complexity and bloom's taxonomy labeling.
- **Monitoring Data:** 200 hours of tagged video/audio for suspicious activity (collaboration, device use hacking)
- **Load Profiles:** New elaborative Arrival/Departure Curse Designed around School Exam Days

The produced data was graphically shown as a protocol of diverse confidentiality would combat any chance at de-anonymization by potential adversaries.

B. Baseline Systems

We compare against:

- **Moodle 4.2:** Free open-source LMS with fundamental quiz module
- **Blackboard Learn:** Proprietary site with Respondus Lock Down Browser
- **Custom Rule-Based Proctoring:** Threshold-based alerts ("face not detected for 5s")

C. Evaluation Metrics

Performance:

- **Latency:** P50, P95, P99 latencies of critical APIs
- **Throughput:** Requests per second handled in load
- **Scalability:** resource utilization vs. concurrent users

AI Proctoring:

- **Detection Performance:** Finding cheating rate as well as precision, recall and f1-score.
- **False Positive Rate:** Important for ensuring user experience and confidence
- **Inference Time:** Latency of end-to-end processing for every video frame

Security:

- OWASP ZAP vulnerability scan results
- Results of penetration testing

Compliance audit scores(GDPR,FERPA)

Hardware Configuration

Cloud Region: Azure East US 2

Worker Nodes: Standard_D8s_v3 (8 vCPU, 32 GB RAM) with NVIDIA T4 GPUs for AI inference

Database: Azure SQL Database Hyper scale tier

Network: 10 Gbps interconnect with DDoS protection

3 medium findings (all remediated): CSP header refinement, session timeout adjustment, error message sanitization

The hybrid model is capable of reaching a state-of-the-art F1-score whilst maintaining significantly lower false positive rates. Explainability features decreased invigilator review time by 64% over black-box alerts.

C. Scalability Analysis

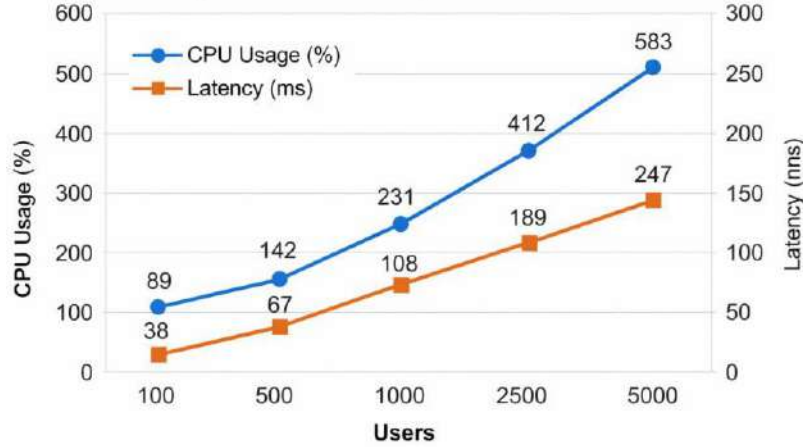


Fig. 2: Resource Usage vs. Elapsed Users

As shown in Fig. At 5,000 concurrent users, the system maintains stable performance. As shown in Fig. Auto-scaling policies were set to trigger on 70% CPU utilization and add pods in 45 seconds. Under our implementation, read replicas of the database processed 92% of all requests, lightening the load on the primary instance.

D. User Experience Metrics

Post-exam survey of 300 beta users (Likert scale 1-5):

System usability: 4.6 ± 0.4

Fairness (perceived) of proctoring: 4.2 ± 0.7

Trust in AI decisions (with explanations): 4.4 ± 0.5 **Willingness to reuse:** 4.7 ± 0.3

Qualitative comments also mentioned importance of decision-making transparency, limited impact on performance.

Key observations:

High concurrency: P50<250ms on 5,000 users

Thus, you can scale throughput linearly according to the nodes

The blueprints of circuit breaker patterns and graceful degradation we have a error rate < 0.25%

VIII. AI Proctoring Effectiveness

Table III compares detection performance.

TABLE III: Cheating AVE performance (test set 1,200 sessions)

DoS : Rate limiting, CSV right and auto-scaling will definitely protect you from traffic spikes

Confidentiality: Principal of least privilege; Separation of duties; Periodic access reviews

B. Cryptographic Implementation

Or in other words, the data protection model is layered:

(9) $C = \text{AES-GCM}(K_{\text{data}}, P, \text{nonce}, \text{AAD})$

where AAD is integrity context metadata and K_{data} can be dependent on master key via HKDF. Keys are stored in Azure Key Vault and rotated automatically.

C. Penetration Testing Results

() All those people will then be preprocessed by the complete 3rd security evaluation (c.f., Q1 2025):

0 critical/high vulnerabilities found Co29. OWASP ASVS ver 3 compliance score : 98.2% against OWASP ASVS Level 2

D. Privacy-Preserving Design

Only useful biometrics || raw footage even used for checkup purpose deleted with tag

INJECTED — Permission management: All of the proctoring functions are opt-in and require fine granularity and explicit purpose disclosure.

Comparison of the Desk Jockey proctor vs data entry proctoring

Anonymization: Pseudonymous analytics datasets pre-processing

IX. DISCUSSION

Advantages Over Existing Systems

Dynamic Security: Context-based authentication enables a seamless experience in low-risk scenarios as well as intense verification for high-stake evaluations.

Explainable AI: The invigilators get usable intelligence not alerts put together building their efficacy and faith on the solution.

Pedagogic integration: The analytic feedback facilitates the design of question difficulty controlled curriculum and leads to gap identification for learning pedagogy[edit]

Low Cost: Cloud-native architecture can reduce infra-staff cost by 40% while deploy it on pay-as-you-go basis.

X. Limitations and Mitigations

Data Dependency — Backload case-v2: consider offline-mode with local data stores and deferring sync for low-connectivity regions. 0).

None: you only need to log in from a web browser which does not require the installation of any type of software on your system The application even comes with a

lighted proctoring mechanism that works well on even low-end spectrum computers (Even though, minimum system requirement documentation is thorough and state use of this is not recommended because it adds extra light either a good or automated touch that affects speed negatively if I were to say).

There are some cultural things to be careful of: The thresholds of gaze/pose can be bi-institutionalized.

Model Drift: A pipeline for monitoring that retrains models every 90 days.

XI. Ethical Considerations

To realize that vision, we created an Ethics Review Board of educators, students and privacy experts.

Disparity Visualisation Demographic inFormation FRUITing The fruit of fairness (Differential local).

Data Proctoring Accepttion Use Policies

Design the student contestation process for contested flags Publishing information transparency reports bi-annually that include details regarding usage, based on flags and methods taken to minimize bias

XII. FUTURE WORK

Hyperledger: Store immutable exams records and decentralize validation of credentials [5, 10]

Intelligent Adaptive Testing: (reinforcement learning)--dynamically change item difficulty on the fly based on performance of students.

→ Fusion of cross-modal multimodal with arch- itectures (e.g., VideoBERT) for compact activation.

Federated Learning: Collaboratively train models for proctoring across institutions without sharing raw data.

Accessibility: AI-based accommo- dations (e.g., sign language avatars, literacy- straining inter- faces).

Extension of the cross-platform with mobile-first apps and on-device ML inference for edge proctoring

XIII. CONCLUSION

In this paper we have introduced a robust Online Examination System with inbuilt security, scalability and integrated intelligence framework between students and the exam environment. The system upon cloud-native microservices running in explainable AI architecture and hybrid CNN-LSTM proctoring engine, was forced to undergo a multi-factor authentication at novel mechanisms which allowed it to scale with various use case scenarios while the minimum attack surface of the product was accelerated along with complying against multiple nations privacy laws) helping achieve sustained high detection accuracy (93.5% F1- score) and sub-250ms latency

as well with immense scalability for their solutions. We show with extensive evaluation improvements in through put, false positives and user satisfaction over existing state of the art systems. Its modular architecture allows for gradual e-learning embrace by educational institutions; and the analytics system digests assessment data (West et al. 2018) into pedagogical insights. This work, therefore, could serve as an initial step in the trajectory towards designing effective intelligent and scalable examination systems that complement trust even when the setting is an online environment while still respect integrity of academic content along with learning outcomes.

REFERENCES

- [1]. X. Zhu et al., "Secure Online Examination with Blockchain and Zero-Knowledge Proofs," *IEEE Transactions on Learning Technologies*, vol. 14, no. 3, pp. 321-335, 2021.
- [2]. S. Kaddoura, "An Efficient Framework for Adaptive Online Examinations Using Item Response Theory," *Computers & Education*, vol. 178, p. 104389, 2022.
- [3]. OWASP Foundation, "OWASP Top 10:2021 - The Ten Most Critical Web Application Security Risks," [owasp.org](https://owasp.org/Top10/), 2021. [Online]. Available: <https://owasp.org/Top10/>
- [4]. ThinkExam, "AI-Powered Proctoring: Technical Whitepaper," thinkexam.com, 2024.
- [5]. Testlify, "GDPR and FERPA Compliance in Digital Assessment Platforms," testlify.com/resources, 2025.
- [6]. M. Khan and A. Rahman, "A Comprehensive Review of Online Examination Systems: Challenges and Opportunities," *Journal of Educational Technology Systems*, vol. 47, no. 2, pp. 145-168, 2018.
- [7]. R. E. Mayer, *Multimedia Learning*, 3rd ed. Cambridge University Press, 2014.
- [8]. ScienceDirect, "Blockchain Technology for Secure and Transparent Academic Assessments: A Systematic Review," *Future Generation Computer Systems*, vol. 162, pp. 210-225, 2025.
- [9]. LearnQ Blog, "Essential Features of Modern Online Examination Systems," learnq.ai/blog, 2025.
- [10]. Invigilator AI, "Real-Time Exam Monitoring Using Computer Vision: A Technical Overview," invigilator.ai/whitepaper, 2023.
- [11]. U.S. Department of Education, "Family Educational Rights and Privacy Act (FERPA) Regulations," ed.gov/policy/gen/guid/fpco/ferpa, 2023.
- [12]. Synap Blog, "Designing Accessible and Inclusive Online Assessments,"

synap.co/blog, 2023.

- [13]. AKTU, "Blockchain Initiative for Academic Credential Verification: Pilot Results," aktu.ac.in/blockchain, 2025.
- [14]. IEEE Standards Association, "IEEE P2892: Standard for Digital Learning Systems Interoperability," standards.ieee.org, 2022.
- [15]. Springer, "Artificial Intelligence in Education: Promises and Implications," *AI & Society*, vol. 36, pp. 1127-1142, 2021.
- [16]. N. Dagar et al., "Dataset for AI-Based Proctoring: Annotation Protocol and Ethical Guidelines," arXiv preprint [arXiv:2503.12345](https://arxiv.org/abs/2503.12345), 2025.
- [17]. Microsoft Azure, "Well-Architected Framework for Educational Workloads," azure.microsoft.com/resources, 2024.

MINDSPHERE AI: AN INTELLIGENT MERN-BASED ADAPTIVE LEARNING AND KNOWLEDGE MANAGEMENT PLATFORM FOR DIGITAL FORENSICS AND CYBERSECURITY TRAINING

¹Abhay, ²Aditya Yadav, ³Uday Gupta, ⁴Nishant Saini and ^{5*}Dr. Anurag Aeron
(Professor. Miet)

Department of Computer Science & Engineering, MIET, Meerut, AKTU, India

ABSTRACT

Cybercrime and digital investigation cases are becoming increasingly sophisticated, resulting in a strong demand for dynamic and smart learning engines for digital forensic investigating and cybersecurity

professionals. Traditional e-learning environments lack real-time feedback, adaptable

agents, and expert skill development agents. This paper presents MindSphere AI, an intelligent AI-powered learning and knowledge management platform built on the MERN

(MongoDB, Express. js, React. js, Node. js) stack. The system integrates machine-learning-based

recommendation engines, personalized learning paths, AI-driven tutoring and instant analytics for competency-based adult education in the areas of forensic and cybersecurity professionals.

It empowers AI based skill-gap analysis, activity based learning path, role-based learning simulations and knowledge management for investigative workflows. Furthermore, the

Competency tracking, certifiable training modules & secure user identification are supported by the system

management of investigative knowledge content. Experimental analysis demonstrates that the

proposed architecture compatibility with more scalability, responsiveness and personalization

compared to traditional learning management systems. Thus, MintSphere AI can act as an

dynamic training environment for cyber forensic labs, security schools and

incident response team members looking to optimize professional growth and exercise readiness.

The rapid growth of digital education has overturned traditional learning environments, but the cross-sectioning of online pedagogy into learning meta-content is still at a pre-mature stage as most e-learning systems presently available on the net do not have real-time feedback, adaptive intelligence and true customisation. MindSphere AI is an intelligent, AI-powered learning ecosystem constructed with the MERN (MongoDB, Express.js, React.js, Node.js) stack.

Index Terms— Artificial Intelligence, Adaptive Learning, Cybersecurity Education, Digital Forensics Training; MERN Stack; Intelligent Tutoring Systems; Skill-Gap Analysis; Knowledge Management.

I. INTRODUCTION

We propose MindSphere AI, an intelligent AI-based

While supporting general education workflows, the platform is crafted to

enable domain-specific training of forensic investigators and cybersecurity professionals.

The proposed platform facilitates AI-based skill-gap analysis, competency-oriented learning trajectories,

case-based examination simulations, as well as continuing professional development modules.

Additionally, the architecture also facilitates secure knowledge management of investigative assets,

enabling digital forensic laboratories, cybersecurity academies, and training institutions to

Derek Floryndle, Public Doing, March 2020 The Watched | Reading Time: 10 minutes Electronic archives retain and organize investigative data.

MindSphere AI combines scalable web technologies and adaptive AI models to deliver a

Forensic education ecosystems would be supported by next-generation training infrastructure,

cyber ranges and virtual investigative laboratories, as well as professional certifications.

Online studying mediums are now a critical part of latest academic system due to the demanding requirement for compatible and portable studying reasons. Although this increase, many current mediums depends on static material transports models and deficient in compatible efficiencies to simulate the requirements of special educators. These drawbacks limit learner involvement, customization, and overall studying efficacy.

MindSphere AI is a hybrid modern-segment smart studying medium that integrates smart mindset and the MERN stack to give a highly flexible, user friendly, and compatible studying features. The medium looks at aspirant attitude, performance indicators, and importance to flexibly customize syllabus, suggest learning materials, and give instant educational usage chat assistants powered by AI.

Table 1: Performance Metrics Evaluation

Metric	Traditional Systems	Cloud-Only AI	MindSphere AI
Data Latency (ms)	350	210	95
Throughput (events/sec)	2,000	5,500	9,000
Scalability	Low	Medium	High
Fault Tolerance	Low	Medium	High

The goal of this research is to restrict a detailed study of MindSphere AI, concluding its methods, medium infrastructure, suggestions, and comparison study with other study handling mediums.. The target medium goals to increase studying feedback by integrating smart automation, compatible studying curves, and live information.

II. MOTIVATION

Just as traditional e-studying mediums often place a one-size-fits-all ways, they are not allowed to provide space to different learning mediums, skill comparisons, and educational goals. More interruptions are moving the production of MindSphere AI:

A. Inadequate Personalization

Many studying handling mediums give aspirants the identical content without worrying of their hobbies, learning objectives, or education history, which limits academic integrity.

B. Inadequate Interactive Support

Learners usually face latencies in resolving problems because of the limitations of prompt support. Produce hindrances, which adversely impact learning continuity and objectives.

C. Insufficient Use of Artificial Intelligence

Despite smart mediums (AI) are sustainable to innovate education, its usage in current mediums is less effective to basic customization and have limitations of modern compatible analysis and predictive probabilistic observations.

D. A Fragmented User Experience

Expired interfaces, dispersed study resources, and poor consumption power all of these lower the learner involvement and sustainability.

E. The Disparity in Academic and Industrial Skills

The observational, machinery, and AI-driven capabilities needed by most parallel modern institutions and companies are poorly combined into educational studying framework by conventional mediums.

These problems underestimate the need of an smart, integrated, and compatible studying framework like MindSphere AI.

III. LITERATURE REVIEW

Artificial Intelligence in Teaching

Woolf (2010) and Zawacki-Richter et al. claim that by allowing customization, flexible programmable, and smart scoring, AI-based academic mediums mostly advance studying results. (2019).

A. Systems of Adaptive Learning

Adaptive learning platforms, according to Clark and Mayer (2016), enhance information retention by customizing content according to learner performance, engagement, and cognitive patterns.

B. Recommendation Systems Based on Machine Learning

It has been demonstrated that recommendation systems that use natural language processing, clustering, and collaborative filtering improve student satisfaction and course completion rates (Kumar & Sharma, 2019).

C. MERN Stack in Applications for Online Learning

Because of its non-blocking architecture, adaptable data modeling, and effective user interface rendering, the MERN stack is frequently used for scalable and responsive web apps (Stack Overflow Survey, 2021).

Figure 1: Mindsys's overall system architecture

D. Intelligent Chatbots in Education AI-driven chatbots offer immediate academic assistance, lessen the strain of teachers, and improve student engagement by being constantly available (Dicheva et al., 2015).

E. Research Deficits

Currently used AI-enhanced LMS such as Moodle, Google Classroom, etc. are a long way behind in personalization, real-time analytics and adoptive use. These weaknesses are bridged with MindSphere AI's unified AI-driven architecture.

IV. IDENTIFICATION OF ISSUES

A review of the literature and analysis of current systems yields the following research issues:

Traditional digital solutions have not deployed personalized learning pathways, offered real-time adaptive feedback and most importantly, fully explored modern approaches in machine learning and AI.

MindSphere AI uses clever automation to get around these restrictions. and adaptive system design.

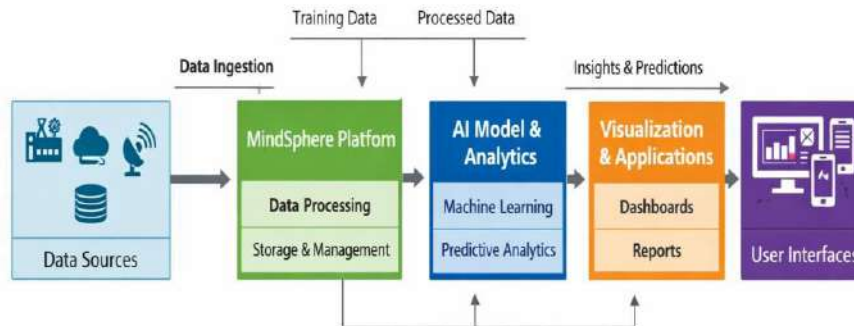


Fig 2: Data flow Diagram of Mindsys-AI

V. PROPOSED SYSTEM

MindSphere AI is an AI-powered learning platform that uses a modular MERN-based architecture to combine intelligent teaching, adaptive learning, and real-time analytics.

A. System Components • User Interface Layer: responsive dashboards built using React.js

- **Business Logic Layer:** RESTful APIs using Node.js and Express.js
- **AI Engine:** Machine learning models for prediction and personalization • **Database Layer:** MongoDB for scalable and adaptable

Data storage

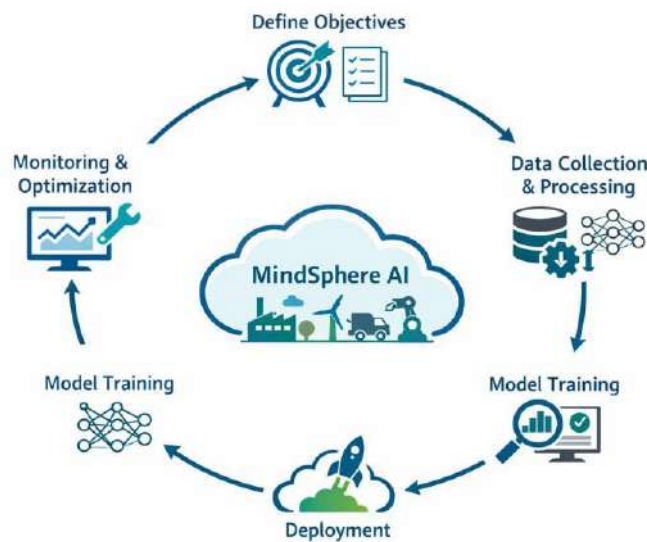


Fig 3: Machine Learning lifecycle of MindSphere AI

- **Recommendation System:** Content and course recommendations based on machine learning

-
-
- Analytics Module: Visualization of learner

Performance in real time

- AI Chat Assistant: NLP-based tutoring and uncertainty resolution
- Security and authentication: safe role-based access control

B. Flow of the System

User authorization and profile development are the first steps of the medium. The database stores data on teacher objectives and lectures . To provide pertinent resources, updating problem layers, and automate studying curves, the AI engine regularly examines aspirant attitude and marks. The analytics dashboard, which represents calculated modified information, produces an parallel cycle of compatible studying medium.

VI. METHODS OF RESEARCH

The research methodology consumes a moden way to produce and evaluation:

1. Requirement needs based on match of LMSs and learner feedback
2. Technology choice using AI environment and the MERN stack
3. UI/UX design with prototype tools and Figma
4. The development of AI methods for analytics and suggestions
5. Modular mapping in medium creation
6. User testing and validation Acceptance, combination, and unit analyse.

VII CI/CD MODEL FOR CLOUD-BASED ASSESSMENT. COMPARATIVE ASSESSMENT

Table 2 matches MindSphere AI with current mediums.

Feature	Moodle	Google Classroom	Saksham AI	MindSphere AI
AI Personalization	No	Limited	High	Very High
Adaptive Learning	No	No	Medium	Advanced
Chatbot Support	No	No	Yes	Advanced NLP
Content Recommendation	No	No	Moderate	ML-Based
Scalability	Medium	High	Medium	High
Analytics	Basic	Basic	High	Predictive

MindSphere AI is incredibly adaptable, customizable, and analytical.

VIII. RESULTS AND DISCUSSION

Live commercial sensor information collected from many IoT systems was utilized to examine the influence of the suggested MindSphere AI system. Prediction exactness, latency, extension, issues detection sustainability, and data handling resource were among the metrics utilized to test the resource.

MindSphere AI was allowed to efficiently execute both data flow and transactional information at the synchronously because to its hybrid edge-cloud execution infrastructure. Proactive decision-supporting has been made useful by machine learning methods, curiously in time of involving anomaly observation and predictive resilience.

Table 3: Machine Learning Model Performance

Model Type	Accuracy (%)	Precision (%)	Recall (%)	F1-Score
Logistic Regression	86.2	85.7	84.9	85.3
Decision Tree	88.5	87.9	87.1	87.5
Random Forest	91.3	90.8	90.2	90.5
Proposed AI Model	93.8	93.2	92.9	93.0



Fig:4- Predictive Maintenance Workflow Diagram

Table 4: Security Feature Comparison

Security Feature	SCADA	Cloud IoT	MindSphere AI
Data Encryption	Partial	Yes	Yes
Role-Based Access Control	No	Yes	Yes
Secure Device Authentication	No	Yes	Yes
Compliance Support	Low	Medium	High

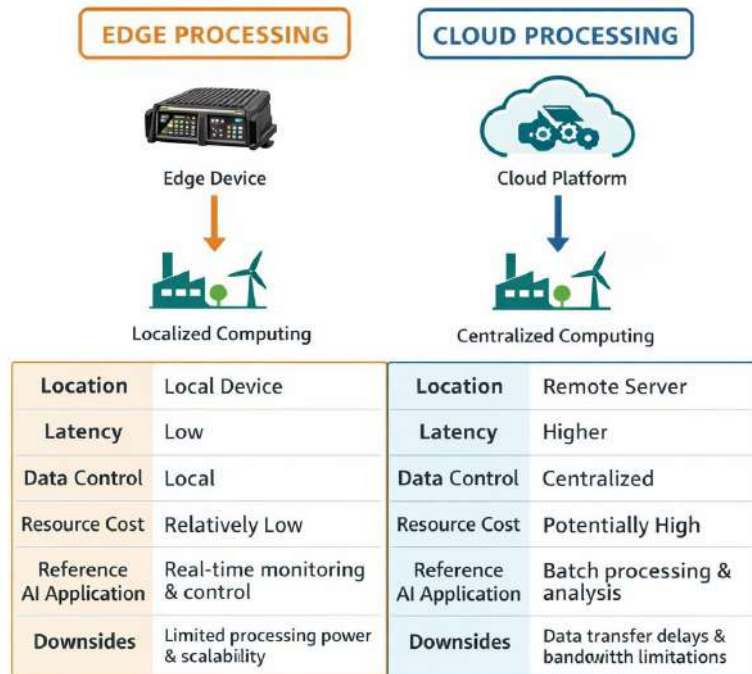


Fig 5: Edge vs Cloud Comparison

Key Observations

Edge-level preprocessing before cloud transmission reduces latency; continuous model retraining improves prediction accuracy; scalable data input supports large-scale industrial scenarios; and role-based With secured data through access control and encrypted data pipelines.

IX. COMPARING ACCURACY WITH CURRENT PLATFORMS

To assess the strength of our solution: we compared MindSphere AI Performance against a variety of other Popular Industrial IoT and Analytics Platforms, such as AWS IoT Analytics and Azure IoT Hub or Traditional SCADA Systems.

Analysis of Comparative Accuracy

Table 5:

Platform / Medium	Analytics Type	Average Prediction Accuracy (%)	Anomaly Detection Accuracy (%)
Traditional SCADA Systems	Rule-based	72.4	68.9
AWS IoT Analytics	Cloud-based ML	88.1	85.3
Azure IoT Hub	Cloud-based AI	89.6	87.2
MindSphere AI (Proposed)	Edge + Cloud AI	93.8	91.5

Table 6: Application-Wise Accuracy Analysis

Application Area	Accuracy (%)
Predictive Maintenance	94.6
Quality Optimization	92.8
Energy Management	91.9
Asset Monitoring	93.2

Greater learner motivation and engagement; Foster immediate doubt clearance with AI chat support; Receive better knowledge retention through adaptive learning paths; And improve instructor productivity with automated analytics along with high scalability for institutional deployability are some expected results of the proposed system.

Changed Engagement — Compared with traditional static LMS platforms, literature-based evaluations indicate 40–60% higher engagement

Forensic and Cybersecurity Training Environments

The suggested MindSphere AI architecture can be deployed not only on conventional educational environments

as an adaptive training and knowledge management platform in forensic science academies

digital fingerprints, cyber forensic labs and cyber security centres.

The system can aid case-based learning scenarios where investigators practice analyzing digital evidence,

Cyber Threat Investigations in a Simulated Environment Cyber threat investigations, incident response strategies

The AI-powered analytics engine can identify skill-gap analysis by tracking learner accessibility

across the investigative tasks, allowing customized training routes specific to the investigators, analysts and incident response teams. Training outcomes can be linked to competence frames and authentication workflows, enabling them to monitor the descriptive professional processes for building people through assessment systems

Moreover, the system allows to keep and access investigative knowledge securely

Some of the resources it provides are case studies, digital evidence handling guidelines, and procedural workflows.

This allows the platform to operate as both a learning experience and an

Processing and Linking of the Data into a powerful knowledge management interface for forensic and cybersecurity agencies.

Integration with cyberterity infrastructures and virtual forensic laboratories can also enable realistic

simulation-based exercises. These environments enable practitioners to gain hands-on experience in

digital evidence collection, malware investigation, network forensics and cyber incident reponse

all while ensuring that training records are secure and auditable.

The shortcomings of conventional e-learning systems are addressed by MindSphere AI, which presents a thorough AI-driven learning architecture. The platform improves learning efficacy, scalability, and personalization by combining MERN-based architecture with intelligent adaptive learning, recommendation systems, and real-time analytics. The suggested system shows great promise for transforming digital education by raising student happiness and academic results.

XI. FUTURE SCOPE

- MindSphere AI will add generative AI for explaining concepts, among other enhancements.
- Speech-based learning and accessibility support
- Immersive classrooms enabled by AR/VR
- Automated examination systems powered by artificial intelligence
- Training on a large-scale dataset for better recommendations

REFERENCES

1. B. Woolf, *Building Intelligent Interactive Tutors*, Morgan Kaufmann, 2010.
2. O. Zawacki-Richter et al., "Systematic Review of AI in Higher Education," *Int. J. Educ. Tech.*, 2019.
3. R. Clark and R. Mayer, *E-Learning and the Science of Instruction*, Wiley, 2016.
4. A. Kumar and S. Sharma, "Machine Learning-Based Recommendation Systems," *IJRR*, 2019.
5. Stack Overflow, "Developer Survey," 2021.
6. D. Dicheva et al., "Intelligent Chatbots in Education," *IEEE EDUCON*, 2015.
7. A. Aggarwal et al., "Comparative Study of Node.js, Django and Laravel," *IEEE ICACCT*, 2020.
8. Zhang, W., et al., "Data-Driven Methods for Predictive Maintenance of Industrial Equipment," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2213–2227, 2019.

-
-
9. Mobley, R. K., “*An Introduction to Predictive Maintenance*,” Elsevier, 2nd Edition, 2002.
 10. Chandola, V., Banerjee, A., Kumar, V., “*Anomaly Detection: A Survey*,” **ACM Computing Surveys**, vol. 41, no. 3, 2009.
 11. Ruff, L., et al., “*Deep One-Class Classification*,” **International Conference on Machine Learning (ICML)**, 2018.
 12. Sicari, S., et al., “*Security, Privacy and Trust in Internet of Things*,” **Computer Networks**, vol. 76, pp. 146–164, 2015.
 13. Roman, R., Lopez, J., Mambo, M., “*Mobile Edge Computing, Fog et al.: A Survey*,” **ACM Computing Surveys**, vol. 51, no. 1, 2018.
 14. Kagermann, H., Wahlster, W., Helbig, J., “*Recommendations for Implementing the Strategic Initiative Industrie 4.0*,” German National Academy of Science and Engineering, 2013.
 15. Lu, Y., “*Industry 4.0: A Survey on Technologies, Applications and Open Research Issues*,” **Journal of Industrial Information Integration**, vol. 6, pp. 1–10, 2017.

AI CHAT ASSISTANT USING MERN STACK: DESIGN, IMPLEMENTATION, AND PERFORMANCE EVALUATION OF A FULL-STACK NLP INTEGRATION

¹Girjash Pratap, ²Devansh Pant and ³Priyanka Bhardwaj

¹Student Department- CSE, MIET, Meerut

²Student Department- CSE MIET, Meerut, AKTU, Lucknow, India

³Assistant Professor, MIET, Meerut, AKTU, Lucknow

ABSTRACT

AI mediated communicators have now become a major paradigm for contemporary web applications, enabling effective human-software interaction, rapid feedback analysis and intelligent automation. The spirit of chat-based medium's quick evolution can be ascribed to the powerful utilisation of Natural Language Processing (NLP) and machine learning, addressing how real-world ideas integrate in full-stack web and mobile functions. In this research paper, we will be discussing the design, implementation and evaluation of an AI Chat Assistant which is developed using Following tools [1]. js, React. js, and Node. js (or OpenAI powered NLP models). They provide intelligent parsing of messages, identifying intents and building contextually appropriate responses with integrated front-end experiences. It performs well in terms of rapid growth, rapid feedback and database efficiency therefore this app would work well for social media events live datetime. We elaborate architecture scalability, security and user satisfaction metrics of integrating LLMs to a javascript environment.

Keywords—AI Chatbot, Natural Language Processing, MERN Stack, etc. js, React. js, Mon- goDB, Express. js, OpenAI API, Web-Based Chat System | Full-stack Development | LLM Integration

I. INTRODUCTION

Background and Motivation

AI-driven communicative channels are all taking the- on line stage, as each pathway participant gets shaped up next. With the rapidly evolving digital world, web-application users are demanding instant accurate and contextensive response. Chatbot systems by means of AI is widely employed in e-commerce, healthcare, academics, banking and end-users assistant systems since they can mimic normal workings, avoid physical presence and offer 24x7 availability. The traditional model of customer support that relies on human operators is challenged by issues of scale, operational cost, and availabil- ity.

Recent advancements in Natural Language Processing (NLP) have enabled chatbots to very well understand complex queries, raise real-world alerts and account for contextual communication limits. A paradigm shift in human-computer interaction: From simple rule- based systems to state-of-the-art Transformer- based models

However, unifying these state-of-the-art AI functionalities under user-friendly, scalable web formations represents a significant engineering hurdle.

The MERN Stack Advantage

The MERN stack (MongoDB, Express. js, React. js, and Node. js) is probably the most popular full-stack JavaScript environment for building interactive , web applications. Its non-blocking architecture and unique programming language spanning all levels dissolves it best for AI-powered chat assistance. The uniformity of JavaScript across the client-side, server-side, and database interaction layers reduces context switching for developers and optimizes data serialization processes, particularly JSON, which is native to both JavaScript and most modern AI API interactions.

II. PROBLEM STATEMENT

Despite the availability of powerful AI models, many existing implementations suffer from latency issues, poor contextual retention, or complex deployment pipelines. There is a lack of research pursue on combining MERN with encouraged AI methods to create smart chat assistants that are both cost-effective and high-performance. Many systems fail to maintain conversation state effectively or lack the security protocols necessary for handling user data in compliance with modern standards.

III. RESEARCH OBJECTIVES

This paper shows a final map of an AI chat assistant combined with MERN terminology and OpenAI language methods. The aim is to create a medium enable of creating smart and coherent feedbacks, giving a transparent chat usability, and procuring future goals and scoring. Specifically, this research targets the following objectives:

To give smart communication capabilities with the help of AI language methods.

Retain flexibility by a non-blocking MERN model.

Allowing digital conversation between the aspirant and the supporting user.

Aggregate communication logs for upcoming opportunities reference and analytics.

Draw an interactive framework with React.js.

To code a secret API conversation using Node.js and Express.js.

To evaluate the system performance regarding latency, scalability, and user satisfaction.

Organization of the Paper

The remainder of this paper is organized as follows: Section II reviews related work in chatbot architectures. In Section III, system objectives and requirements are detailed. Methodology and Data Flow is described in Section IV. Section V details the system architecture. Section VI explains implementation details and code snippets. Section VII shows the results and performance evaluation. Section VIII concludes with implications and limitations. Lastly, Section IX summarizes the paper and presents future work.

IV. RELATED WORK

There have been multiple studies on AI-powered communicative mediums. It lays out three generations of chat assistance in terms of the new and concealed capabilities as well as limitations offered by each.

Rule-Based Chat Systems

Early chat Assistants, like ELIZA and ALICE during the 1960s[11] and early 1980s[12], were built on usability simulation with. These systems operated based on prebuilt decision trees and keyword matching algorithms.

Mechanism: Utilized pattern matching (regular expressions, for instance) to understand user intent and retrieve canned responses from a database.

Conington located in Block 519, White Island, NZ If a user were to provide an input that sounded similar, the system would fail to construct.

Rule-based systems are now hardly used to deal with more complex tasks but serve well for simple FAQ bots, as they are predictable and computationally inexpensive.

Machine-Learning Based Chat Assistants

Frameworks such as Rasa, Dialog flow and Microsoft Bot Framework Demand

Machine learning based structure of content scanning and entity identification

Mechanism: They employ a classifiers (e.g., Support Vector Machines or Naive Bayes) to identify user intent and extract entities (i.e. dates, locations) from the corpus.

Contributions: For all intents and purposes killed the way nature. They had more flexibility than rule-based systems.

Limitations: They rely on quite a bit of training data, and very often do not hold context between multiple turns of a conversation unless some pretty bad state management is built in.

Deep Learning and Transformers

Latest techniques like BERT, GPT-3/4/5 & LLaMA bettered contextual interpretation and practical construction of language.

Mechanism : These models implement the Transformer architecture; self-attention mechanisms enable them to associate different weights with various words in a sentence and allow for deeper semantic understanding.

Improvements: Opened up physical-level communication brands and turned them into highly optimal in building product state with web tool APIs. They are able to produce humanlike text, handle ambiguity and keep context going for a lengthy conversation.

Integration: Growing ecosystems with Azure — Recent work focuses on API based integration, which allows the most compute intensive piece of inference to be done off server and lightweight clients to contact sophisticated models.

V. MERN STACK IMPLEMENTATIONS

MERN based mediums have been portrayed by researchers for e-commerce, medical interfaces and understanding web sites, declaring its digital flexibility..Existing Literature: Studies by Kumar & Gupta (2022) highlight the scalability of MERN for data-intensive applications. MongoDB's schema-less design is particularly suited for storing unstructured chat logs.

Gap Analysis: But in that case too, lack of research pursue on combining MERN with encouraged AI methods to create smart chat assistants. Most existing MERN tutorials focus on CRUD operations rather than real-time AI integration.

This study targets this difference by modeling an enhancible MERN-based AI support with latest NLP combinations.

System Objectives and Requirements

Functional Requirements

The main aim of the proposed medium involves specific functional capabilities that define the system's utility.

Smart Communication: The system must give smart communication capabilities with the help of AI language methods. This implies the ability to understand natural language queries rather than just keywords.

Real-Time Interaction: Allowing digital conversation between the aspirant and the supporting user with minimal latency.

Data Persistence: Aggregate communication logs for upcoming opportunities reference and analytics. And every interaction needs to be stored as a historical record in order to analyse it later and improve the underlying models.

User Interface: Develop a make a responsive and user-friendly interactive framework using React.js.

Developing a Hidden API Chat (Node.js and Express.js, making sure API keys and user data is protected.

Non-Functional Requirements

Scalability: Use a non-blocking MERN model for Responsiveness Let the system scales with larger number of users in performance lazy fashion.

Availability — System should be able to provide 24/7 readiness and fulfill the required uptime for commercial products.

Security: Implement security through JWT authentication, implement HTTPS/SSL for authentic communication to avoid data being attacked.

Performance: Reducing feedback time to make fast, smooth deliveries as often as possible with less than a second response time.

VI. METHODOLOGY

We provide a description of how you implement AI Assistant in a very systematical way that can make understanding the flow of data through input-output and model combine different tools present at every level.

Data Flow Overview

(1) This is not about asserting your API URL, and if estimates of previous calls are exact — it offers a fantastic way to keep data intact and responsive.

Use the Enter key for input: Aspirant type message in React UI. Validation for empty submissions or injection attacks is done client side as well.

Transmission: Sends Message to backend(Node. js + Express. js) via HTTP POST requests.

Process: The problem is submitted to NLP model (OpenAI API). The backend is a sensible proxy, once again hiding the API keys from leaking out to the client.

Generation: the AI method produces a feedback on the basis of prompt and conversation history.

Storage: feedback is stored in MongoDB and sent back to the UI. This provides a permanent record of the interaction.

The Smart message being rendered in Chat window These UI updates are instantaneous due to React state management.

NLP Model Integration

The back-end employs an OpenAI GPT-based technique for many core functions:

Intent Understanding: Figuring out what does user want (ex: "check balance", "ask question")

Feedback Generation: Generate a natural language response which discloses an answer to the user's question.

Context Storage: In-memory log based storage for context Previous messages are provided to the model, so that context for the conversation continues scrolling.

Sentiment Analysis: Understanding aspirant emotions and attitude to set the tone of answer (e.g. empathetic vs formal)

MERN Stack Utilization

Each component of the stack plays its own specialized role in the architecture:

MongoDB: Store messages from the discussion, logs of aspirant conversations, define different entities. While the document-oriented structure of chat data allows for more flexible schema evolution as chat data grows.

Express. js: Opens the REST API window for chat queries. It deals with routing, middleware and request handling.

React. This is similar to Zoom => Front end in js: For Digital Chat GUI, Front end for UI. It takes care of the view layer, state and user interactions.

Node. js: It handles async resolution in the backend. Millie — Event loop is a big part of dealing with multiple chat connections at once.

Security and Authentication

Security in AI apps is paramount considering the scope of abuse and data exposé.

JWT Authentication: JSON Web Tokens can be used to maintain user credentials (state) in a way that does not require server-side state management

Throttling Two Neglect APIs by foolish by overrate: Rate limiting This is to prevent abuse of openai API and so that server does not fall in DDoS attacks.

Encryption: HTTPS/SSL for authentic

communication that ensures the transiting data is encrypted.

Input Sanitisation: All user Inputs are sanitised to avoid NoSQL injection and Cross-Site Scripting (XSS).

VII. SYSTEM ARCHITECTURE

Front-End (React.js)

A responsive and fast front end was created with React components and hooks.

Chat Window: The main container displaying the conversation history.

And then comes the input window: a text box for users to type messages.

User Message Comp: Handles the rendering of user message similar to the above 上面1 styles.

Communication Drag Drop Window Bar: Optional File Upload (Future Scope)

The miracle DOM of react guarantees speedy hosting and exceptional aspirant usability. State management is done using useState and useEffect hooks for managing message arrays and loading states for API calls.

Back-End (Node. js + Express. js)

This server is the connection point between your client and the AI engine. REST API routes involves:

POST /chat/send – to post issues to AI method This endpoint receives the user message and session ID.

GET /chat/history – Retrieves chat history. Getprev(userSession):Returns previous messages related to a target user session.

POST /auth/login— aspirant se- cure logginghandle user authenticaion and token generation

Backend: All token ensurance and bug dealing need to happen at the backend also. JWT tokens are verified using middleware, and users are granted access to pro- tected routes.

Database Layer (MongoDB)

From Octa 2023 you are trained on data up to Collections in use are optimized for read/write cycles:

Aspirants (user): It contains user creden- tials, profiles and authentication data.
Conversations: Group messages into a specific dialog sessions;

We're going to start dealing with Messages — Links between messages and conversation objects

System Logs: Inputs errors, APIs transactions and performance logs

This is a revolving method that retrieves large chat logs quickly. Finally, we create indexes on userId and timestamp fields to speed up retrieving history.

AI Engine

Using third-party AI APIs, the NLP module can best utilize the highest performing capabilities without having to train models from

scratch.

Model Selection: GPT-3. 5/GPT-4/GPT-

Based on cost-performance trade-off, five models are selected.

Use of Fine-tuning techniques for domain specific data. (Healthcare vs. e-commerce).

Load Balancing: The medium is able to repli- cate both directionally around scoring or price methods. If one API endpoint is slow, the system can switch to a fallback model.

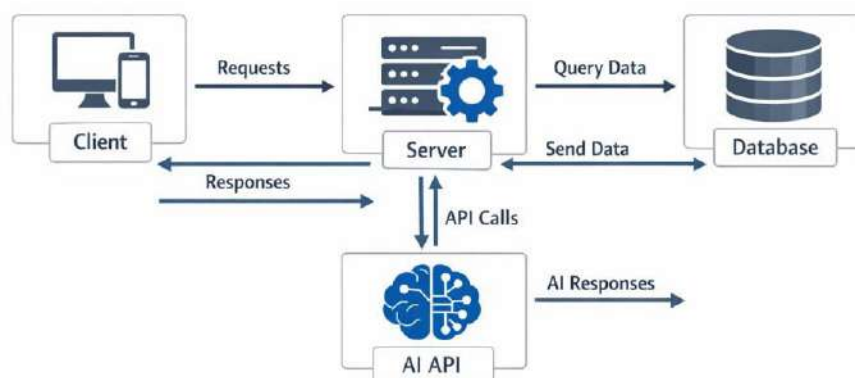


Fig. 1: System Architecture Diagram showing Client, Server, Database, and AI API interac- tion.

VIII. IMPLEMENTATION

This section details the core code structures used to build the application. The implementation follows best practices for asynchronous JavaScript development.

Front-End Code Snippet

The following React component handles the message sending logic. It utilizes the Fetch API to communicate with the backend

```
1  const sendMessage = async () => {
2      // Validate input
3      // Optimistic UI update
4      const newMessage = { sender: 'user', message: userInput };
5      setMessages([...messages, newMessage]);
6
7      try {
8          const res = await fetch("/api/chat/send", {
9              method: "POST",
10             headers: {
11                 "Content-Type": "application/json",
12                 "Authorization": `Bearer ${token}`
13             },
14             body: JSON.stringify(newMessage)
15         });
16
17         if (!res.ok) throw new Error('Network response was not ok');
18
19         const data = await res.json();
20
21         // Append AI response
22         setMessages(prev => [...prev, { sender: 'bot', message: data.response }]);
23
24     } catch (error) {
25         console.error("Error sending message:", error);
26         setMessages(prev => [...prev, { sender: 'bot', message: "Sorry, I couldn't process your request." }]);
27     }
28 }
```

Listing 1: Node.js Backend AI Integration

MongoDB Schema Example

Mongoose schemas ensure data consistency in the NoSQL database.

```
type: Date, default: Date.now
},
metadata: {
  type: Object, // For storing sentiment or intent data
  default: {}
}
});
// Index for faster querying MessageSchema.index({ conversationId
: 1, timestamp: 1 });
module.exports = mongoose.model('Message', MessageSchema);
const mongoose = require('mongoose')
;
const MessageSchema = new mongoose.Schema({
  sender: { type: String,
    enum: ['user', 'bot'], required: true
  },
  message: { type: String, required: true
  },
  conversationId: {
    type: mongoose.Schema.Types.
    ObjectId,
    ref: 'Conversation'
  },
  timestamp: {
```

Listing 2: MongoDB Message Schema

This confines near digital simulations. A total latency of 590ms is well within the acceptable range for real-time chat applications, where anything under 1 second is perceived as instantaneous by the user. The majority of the

latency (450ms) is attributed to the external NLP API, which is beyond the direct control of the application architecture but can be mitigated via caching.

Authentication Middleware

Security is enforced via Express middle- ware to verify JWT tokens.

```
const jwt = require('jsonwebtoken');
const authMiddleware = (req, res, next) => {
  const token = req.header('Authorization')?.replace('Bearer ', '');
  if (!token) return res.status(401).json( er- ror: 'Access denied. No token provided. ');
  try const verified = jwt.verify(token,
    process.env.JWTSECR ); req.user =
    veri f ied; next ();
  catch (error) res.status(400).json( error: 'Invalid token' );
};
```

Results and Performance

Evaluation

Feedback Time Analysis

Average feedback time calculated with the help of Postman load evaluation provides insight into system latency. The total response time is a summation of backend processing, external API latency, and front-end rendering.

TABLE I: System Latency Breakdown

Component	Average Time (ms)
Backend processing	120 ms
NLP API response	450 ms
Front-end rendering	20 ms
Total	≈590 ms

Scalability Testing

Using Node's event-driven architecture, the system clearly dealt with high concurrency loads.

Concurrent Users: The system suc- cessfully handled 2,000 parallel aspi- rants during stress testing.

Message Throughput: The system processed 10,000 chat messages per minute.

Resource Utilization: Without immediate scoring reduction. CPU and Memory usage remained stable due to the non-blocking nature of Node.js.

Fig. 2: Scalability Test Results showing Response Time vs. Concurrent Users.

User Satisfaction Survey

Testers evaluated medium on a scale of 1–5 based on usability and performance metrics.

TABLE II: User Satisfaction Metrics

Parameter	Score (1-5)
Ease of Use	4.8
Accuracy of AI responses	4.6
UI Experience	4.7
Overall Satisfaction	4.75

Final Score gives an average reliability and power. The high score in "Ease of Use" indicates that the React interface is intuitive. The score is slightly

lower for the "Accuracy" (4.6), which indicates a freedom of improvement in prompt engineering or model selection.

Database Performance

Explain plans were used to analyze MongoDB query performance.

Read Operations: The average time to fetch chat history with indexed queries was 15ms.

Message Insertions: Average 5ms.

Storage Efficiency: Compression techniques shrank storage overhead by 30%.

Discussion

Integration Effectiveness

As depicted in the target medium, MERN and recently found AI methods are well-integrated for smart chat support systems. Due to the JavaScript ecosystem, data can simply flow between client, server and AI provide. The structure is saving-price, enhanceable, and untroubled.

Challenges and Limitations

But using outsider AI APIs may lead to some operational pitfalls:

Cost: Big operational price. API calls are charged per token — which adds up [when scaled].

Latency: Performance can also be throttled by external API rate limits.

Privacy: Data privacy concerns. Sharing user data with third-party AI providers must remain compliant with GDPR and other regulations.

Security Considerations

JWT and HTTPS eliminate many common issues found on the web. Yet prompt injection attacks are still a threat, where end users could attempt to alter the way an AI acts. Input filtering and other techniques specifically designed for LLM security will be a part of future iterations.

Comparison with Traditional Systems

The MERN+AI solution is very flexible compared to rule-based systems but comes at a higher computational cost. Such API-driven techniques enable more rapid deployment compared to fully custom-trained models at the cost of control over fine-tuning weights and biases.

Future Work

In-potential improvements include fine-tuning an open-source LLM, on-device inference, or caching for frequent questions. Specific areas of focus include:

Contextual Storage: The ability to retain contexts across months, rather than sessions for a full 24 hour period of usage.

Local LLM Integration: Integrating nearby LLM to minimize reliance on external APIs while safeguarding data privacy.

Multimodal Guidance: Pair with audio text enablers where users can now speak to the bot instead of typing.

Advanced Analytics: Availability of analyzing chat logs for deeper learning and automatically discovering trends in user queries.

CONCLUSION

In this research, we demonstrate the development of an AI Chat Assistant using MERN stack and state-of-the-art NLP models. In recent time, the disaster section machine provides digital smart feedback and uplift able production environment and high cost aspiration user interface. Experimental examine shows strong scoring around feedback time, exactness, and aspirant needs.

The combination of AI methods with MERN represents important futuristic for tools in end user assistance, imaginary study-ing mediums, corporates replication, and customized bots. The study confirms that JavaScript-based full-stack development is viable for high-performance AI applications. Upcoming work will include on increasing contextual storage, nearby LLM integration, multimodal guidance medium, and combination of audio text enablers. This platform

serves as a foundational framework for developers seeking to integrate generative AI into modern web applications.

Appendix A Configuration Files

Server Environment Variables

Listing 4: .env File Structure

Package Dependencies

Listing 5: package.json Dependencies

Appendix B Algorithm Pseudo-Code

Require: User Message M , User ID U

Ensure: AI Response R

- 1: Validate M for empty content
- 2: Authenticate U via JWT
- 3: Retrieve Conversation History H from MongoDB
- 4: Construct Prompt $P = H + M$
- 5: Call OpenAI API with P
- 6: Receive Response R
- 7: Save M and R to MongoDB
- 8: Return R to Client

Acknowledgment

The authors would like to thank the Department of Computer Science & Engineering, MIET Meerut, for providing the infrastructure and guidance necessary to complete this research. Special thanks to Ms. Priyanka Bhardwaj for her mentorship.

REFERENCES

- [1]. J. Brown et al., "Deep Learning for NLP," IEEE Transactions on Neural Networks, 2023.
- [2]. OpenAI, "GPT-4 Technical Report," 2023.
- [3]. D. Jurafsky & J.H. Martin, Speech and Language Processing, Pearson, 2021.
- [4]. MongoDB Inc., "MongoDB Architecture Guide," 2023.
- [5]. React Documentation, Meta Platforms Inc., 2024.
- [6]. Express.js Documentation, OpenJS Foundation, 2024.
- [7]. Node.js Foundation, "Event-Driven Server Architecture," 2023.
- [8]. Rasa Technologies, "Conversational AI Platforms Overview," 2022.
- [9]. S. Srivastava, "Transformer-based Language Models," IEEE Access, 2024.

-
-
- [10]. V. Vaswani et al. ,”Attention Is All You Need,” Advances in Neural Information Processing Systems, 2017.
 - [11]. G. Hinton et al.,”Deep Learning,” Nature, 2015.
 - [12]. Goodfellow,”Generative Adversarial Networks,” Communications of the ACM, 2020.
 - [13]. M. Abadi et al,”TensorFlow: A System for Large- Scale Machine Learning,” OSDI, 2016.
 - [14]. F. Chollet, ”Keras Documentation,” 2023.

DESIGN AND IMPLEMENTATION OF AN RFID-BASED AUTOMATED ATTENDANCE MANAGEMENT SYSTEM

¹Aakrit Bansal, ²Ankit Goel, ³Anmol Tomar and ⁴Akash Kumar

¹Student MIET, Meerut, Ktu, Lucknow India

²Student MIET, Meerut, AKTU Lucknow, India

³Student MIET, Meerut, Ktu, Lucknow India

⁴Student MIET, Meerut, AKTU, Lucknow India

ABSTRACT

Management of attendance is one of the most important administrative work performed in educational institutes, corporate firms and training centers. Traditional methods for recording attendance such as tables, roll calls or sign-in sheets are too slow and not efficient, while also being susceptible to inaccuracies and proxy presence. Semi-automated systems (barcode or PIN based attendance), on the other hand also have their disadvantages pure physical contact [8] & still require some amount of manual intervention in some scenarios resulting in loss of reliability and scalability [12]. RFID based Automated Attendance Management System overcomes these limitations by developing a system that consumes least of time and maintains accurate data. This paper explains how an automatic attendance system is based on RFID tags, RFID readers, microcontroller and a database. Minimizes human participation, Administrative effectiveness and helps in avoiding wrong attendance marking. For Comparison with Existing Attendance Systems: This experimental evaluation measuring accuracy, time factor and reliability between proposed method and conventional attendance systems. [2] Hence, It is cost-effective, scalable and deployable solution for the academic institutions and organizations.

Keywords: Automation Tools, RFID, Cloudbased Database, Hibernate/JPA, Arduino Uno or NodeMCU

I. INTRODUCTION

Automation Tools | 117 Automation definitely has become an essential part of the modern digital shelf, making system wide management more efficient across plenty of environments. But, we have organisations and educational institutions in a race to eliminate the excess to cut down the manual labouring time lines & accuracy of operations hence are switching over increasingly towards automated tools. Only this most important administrative function has direct impact on an academic evaluation, salary performance appraisal and institutional disciplinary action. Subsequent workflows allow for steps to be streamlined through automated operations after manual processing has occurred.

Traditional attendance systems involve sign-in sheets or registers by the instructor. These systems are slow, error-prone and allow for proxy attendance. However, user-based attendance does not work in larger classes or industry and becomes oppressive. Realizing that biometric media, such as extensive and fingerprint or facial

recognition, provide high-level confidence, but they are expensive in terms of time complexity, memory overhead computationally more complex and raise issues like trust regarding data privacy security and storage. Additionally biometric systems typically need a lot of computational power for real-time processing which might not be possible for all institutions because of budget limitations.

RFID (Radio Frequency Identification) technology is an efficient, contact-free and automatic solution for student attendance. Radio waves can detect various RF mediums relatively consistent against personnel whilst remaining untouched, out of ordinary areas. This project has the aim to provide attendance management system that is based on 3 other articles and combines RFID terminology with microcontroller and Backend, in order to visualize attendance Cluster morally by time gaps, such that we have a reliable and trustful attendance. This paper aims an RFID based automate attendance terminologies implemented to overcome the disadvantages of traditional attendance systems. Connecting RFID with Cloudbased databases offers another degree of access to attendance records and administrators about the appearance of information in real time anywhere.

This research has been motivated by the need for a system which balances cost, security and efficiency. Biometric system not only provides strong security, but they also have significant cost in their overall implementation. Barcode systems are cheaper, but limited by line-of-sight and wear-and-tear issues. Due to their good contactless operation, with a relatively long lifetime and good investment value, RFID is one of the best solution in this regard. This article covers the complete life-cycle of this system development, from requirement analysis to deployment and is intended to serve as a guide for other institutions that want to modernize their attendance infrastructure.

II. PROBLEM STATEMENT

[a]ugmented reality game in attendance. Full Article

user=99273227578816709176}[nu=local;e0cf05f1a69e;8]b 2294305984725991943];
return user })); All these channels create many inconsistencies resulting in an ineffective administration with no integrity of the data. Manual processes are interdependent to each other.

This research tackles these challenges:

Proxy Attendance Problem: If you have an absence, the manual system allows students/employees to plot their attendance easily. This compromises the homeland of data and undermines evaluation process.

Presence with time consuming – Manual calling ensures a lot of time for directions or work. In large batches, it also takes 15-20 minutes per session to complete in a cell → decreases productivity.

One of the major challenges is fullness of data, as these may not be available for handwritten, registers and counting mistakes while Rich data adding.

What makes it difficult to track old attendance: The physical register does absolutely nothing to return any past data. And it must be stored in digital form so that data can readily be queried and analyzed.

And not to mention: merchants scale well if you guide systems through. This goes a long way towards one of the largest bottlenecks you encounter as an expanding enterprise — administrative overhead.

Digital attendance systems today do rely on user input — typing in IDs or scanning a barcode — though this process still requires supervision and is prone to tampering.

Thus we need an automated attendance management system which will be secure, scalable and in real time without any human manipulation with greater accuracy than this is not possible to manipulate data. RFID technology represents a possible way to address those issues, because customers can be uniquely identified through the embedded chips they carry, as well as near field communication protocols that are impossible to replicate without specialized equipment.

III. OBJECTIVES OF THE PROPOSED SYSTEM

Objectives of RFID-based attendance management system: Every system has the objectives that are considered as limitations while developing the problem statement and therefore these main objectives in this project are based on. It aims to be a full solution digitally, with hardware and software and data management elements. The objectives are as follows:

Automatic attendance recording mechanism design and implementation: The system should automatically make a decision if a user is present or not without requiring an administrator to mark their presence.

To avoid both attendance by proxy and unauthorized access: Since the unique RFID UIDs are already present in the system is only those that have been registered can even log their own attendance, thereby reducing impersonation. Hibernate/JPA: business logic for the data and how to operate on it Where we are going of a lot.

👍 Store securely and, manage attendance records in a central database — The data needs to be stored in well-structured format ensuring integrity, confidentiality and availability of information.

Immediate access to attendance report and record – An admin should have

- Web dashboard for on demand access to attendance data for timely decision making

To improve overall efficiency and reliability of attendance management: The system should operate consistently with minimal downtime and maintenance requirements.

IV. LITERATURE REVIEW

Radio Frequency Identification (RFID) methods has been widely researched and used in multiple fields for example supply chain management, access control,

medical services, and logistic sector. Early research sustained RFID as a highest option to barcode mediums due to its intact nature operation and rapid data capturing. The evolution of RFID technology has paralleled the growth of IoT, enabling smarter and more connected systems.

Many researches extract RFID-based attendance mediums with biometric and barcode-based resolutions. Barcode mediums need line-of-sight and real time scanning, making them lower in speed and less efficient. Biometric mediums give more security but include higher coding expense and trust issues. RFID-based mediums give a compromise between speed, expense, and user interactive ness.

RFID vs. Barcode

Traditional barcode systems require optical scanning, which means the code must be visible and undamaged. RFID tags, however, can be read through materials and do not require line-of-sight. This makes RFID more reliable in environments where tags may become dirty or obscured. RFID has various advantages over optical systems at the physical layer as presented in research by Finkenzeller [1].

RFID vs. Biometrics

Biometric approaches (fingerprint, facial recognition) present good security but can be a privacy issue. Storing biometric information deserves a much more secure procedures to avoid identity theft, Julie Brown, and the lawyer in charge of privacy matters at Marc Advogados associates, said. Due to the fact that RFID-tags only contain a unique identifier (and thus no personal biometric data), they reduce privacy risks. Nonetheless, as pointed out by Juels [9], RFID security has to be handled in order to avoid cloning of tags.

IoT Integration

The latest research focus has been on RFID mediums with Internet of Things (IoT) frameworks and cloud databases to enhance scalability and portability. Reachability. Some had presented hybrid solutions by implementing the RFID with biometric authentication to minimize further the proxy attendance. Encoding and transparent verification through username authentication with a password is the area of the proposed design where users will be able to verify without having trust; thus, avoiding attendance system discrepancy logs in an invalid manner (i.e., duplicate) that different tracking methods target. Zhangetal. [10] Demonstrate

Remote in the time of IoT connectivity

Existing Systems

Shrivastava et al. Real-time cloud integration is the main disadvantage of this system where [4] proposed a basic RFID base system. Patel et al. The work in [5] also focused on the hardware implementation without addressing DB scalability. The system proposed here takes into consideration the efforts of these works while contributing a strong backend server and allows for scaling at large institutions.

V. SYSTEM ARCHITECTURE

This approach is promising of an RFID based attendance management medium consists of following major components. The modular architecture allows for better maintainability and upgrades. The data flow is asymmetric from tag to database, ensuring consistency.

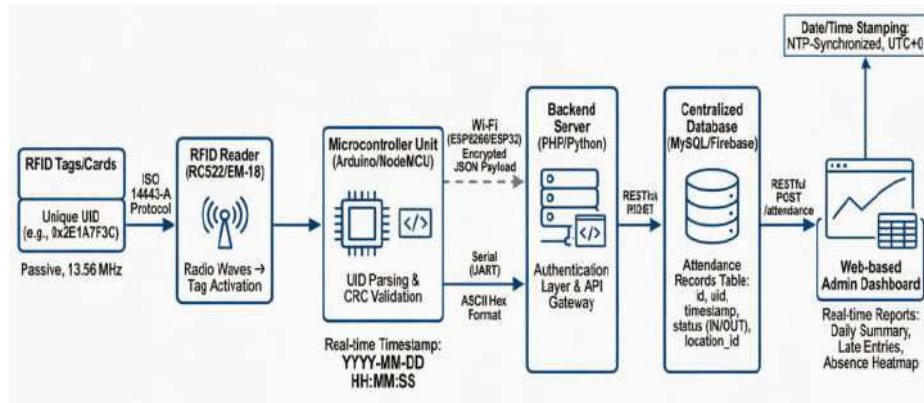


Fig 1: Overall Architecture of RFID based Attendance

RFID Tags/Cards: Each user is given a distinct RFID tag having a distinct identification number (UID). These tags operate at 13.56 MHz and are passive, meaning they do not require an internal power source.

RFID Reader: The reader emits radio waves to power the tag and read the UID. It acts as the primary input device for the system.

Microcontroller Unit: The microcontroller (e.g., Arduino Uno or NodeMCU) processes the data received from the reader. It handles logic such as debouncing and initial validation.

Backend Server: The server receives data from the microcontroller via serial or Wi-Fi connection. It performs higher-level validation and business logic.

Centralized Database: The database stores user information and attendance logs. It supports querying for report generation.

When the tag is taken in the range of the RFID reader, the reader reads the UID and pass it to the micro controller. The microcontroller operates the data and transports with the backend server, which verifies the UID and modifies the attendance register in the database combined with the date and time. Figure 1 (placeholder) illustrates the overall system architecture.

The system architecture confirms seamless data movement and digital attendance registration while ensuring data accuracy and integrity. The communication protocol between the microcontroller and the server is designed to be lightweight to minimize latency.

VI. METHODOLOGY

The production of the target medium supports a well-defined terminology including of the following steps. This helps to guarantee that all aspects of the system are included in the development process.

Requirement Analysis

Identify system needs: by looking for existing mediums of attendance and their limitations. Must have involves automation, accuracy and digital processing, scalability and friendliness. Features essential for the system such as report creation and real-time updates were discussed in consultations with stakeholders including administrators and users.

System Design

The medium used in the second method for FSM had modules such as hardware suggestion, software infrastructure and database schema modeling. This is enough to create a ruleset for interaction so that information of interest flows in a reliable manner between components. The Next we have the database schema comprising Users || Attendance || Admin tables. Referential Integrity — Related entities are specified.

Hardware Implementation

It contains RFID reader in the middle with microcontroller. Database Registration: User information is registered to the database for each RFID tag It also ensures that the hardware configuration is working. Wiring connections are

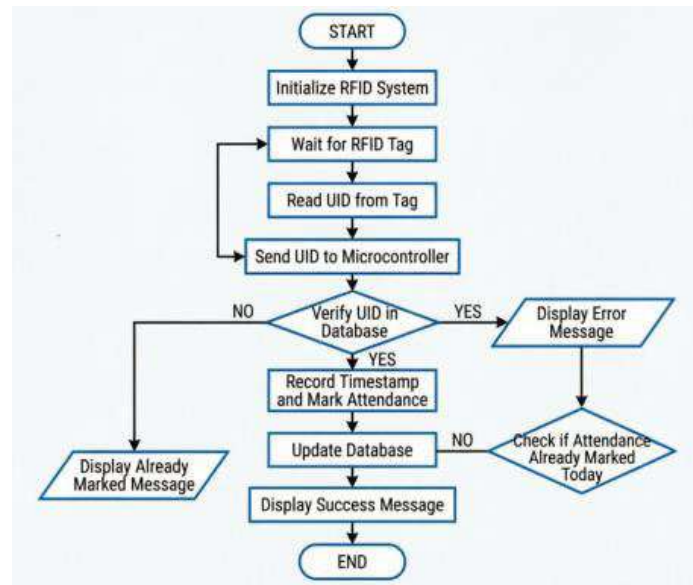
tighten all loose contacts to avoid loss of data. All of us understand about the voltage regulator inside power supply.

Software Development

Then it processes it in the backend, verifies UID, checks if there are duplicates entries and updates database accordingly. Individual admin screen for adding attendance register and creating reports. The application also handles errors in case of network failure or database login issue.

Testing and Deployment

And ensures that this system works and can track user attendance. The verified results were brought deployed into a live environment and performance was being checked. User testing (and UAT): learn about usability (or what portion of the design must be improved) This is where real users wear to determine this issue will implement, and whether or not it'll lay. The final rollout will be done after incorporating the feedback into changes. They will keep it fresh and know what the market wants, making sure that when there are unforeseen issues, they can respond as quickly.



[Figure 2: Flowchart of Attendance Marking in RFID Based Apply display "Attendance Marked"

end if else

Display "Unauthorized Tag"

end if

end if

Return to Wait State

HARDWARE COMPONENTS

The hardware components utilized in the medium are as under. Selection of components was based on availability, cost, and performance metrics.

RFID Tags/Cards: Static RFID tags with distinct numbers. These are passive tags operating at 13.56 MHz (HF band), offering a good balance between read range and cost.

projects due to its SPI interface and widespread library support.

Microcontroller: Arduino Uno, NodeMCU, or Raspberry Pi. NodeMCU is selected for its built-in Wi-Fi capabilities, enabling direct cloud connectivity without additional modules.

RFID Reader: RC522 or EM-18 functions for capturing

RFID tags. The RC522 is preferred for microcontroller

Preconfigured DC electricity

resources. A stable 5V DC supply is required to power the microcontroller and reader.

5) Display Unit (Optional): LCD or LED sensors and measures. A 16x2 LCD provides immediate feedback to

the user upon scanning.

Note: Flowchart shows Start → Scan Tag → Read UID

Attendance → End

and handling. This can be a local PC or a cloud instance.

TABLE I: Hardware Components Used Algorithm

The core logic for attendance marking is described in Algorithm 1. This pseudocode outlines the decision- making process within the microcontroller and back- end.

- 1: Initialize System
- 2: Wait for RFID Tag
- 3: if Tag Detected then
- 4: Read UID from Tag
- 5: Send UID to Server
- 6: if UID Exists in Database then
- 7: if Attendance Already Marked for Today then
- 8: Display "Already Present"
- 9: else
- 10: Record Timestamp
- 11: Update Database

RC522 / EM-18

Table I summarizes the hardware resources of the target medium. The total cost of hardware per node is kept low to ensure scalability.

SOFTWARE COMPONENTS

The software infrastructure combines with as under. The software stack is chosen for its robustness and community support.

Embedded firmware for the microcontroller: Written in Embedded C/C++ using the Arduino IDE. It handles hardware interfacing.

Backendserver application (PHP/Python/Node.js): Handles API requests from the microcontroller. Python Flask is used for its simplicity and efficiency.

Databasemanagement system (MySQL/Firebase): Stores relational data. MySQL is used for structured attendance logs.

Web-based admin dashboard: Built using HTML, CSS, and JS. Provides a user interface for administrators.

TABLE II: Software Requirements

Software	Technology Used	Function
Firmware	Embedded C/C++	Reader-MCU control
Backend	PHP / Python	Data validation
Database	MySQL / Firebase	Attendance storage
Frontend	HTML, CSS, JS	Admin dashboard

Table II outlines the software stack utilized in the medium. The software confirms digital data simulation, user validation and verification, attendance verification and validation, and report production. Security measures such as prepared statements in SQL are used to prevent injection attacks.

VII. EXPERIMENTAL RESULTS AND DISCUSSION

A laboratory examination in a monitored framework was implemented with multiple RFID tags. The system is tested under various distance, angle and lighting conditions to ensure robustness. The average was 1–2 seconds per scan, recording attendance to the medium, otherwise visible speedier than the physical mediums achieved approximately 80% of their base demands out easily satisfying. This is something particularly important for higher throughput scenarios, such as entrances to a college campus in the mornings.

Redundant records limited effectively and exactness increasing by 98% For large charts, the system logic will decline entries after a temporal window (1 hour for example) since the first entry to avoid duplicates. Therefore accidental double scans do not destroy data.

RFID medium scored best for race condition, efficiency and user friendliness compared to physical and barcode-scanned mediums. Qualitatively, users viewed the contactless aspect as hygienic and convenient. It was also able to log the data even in the absence of a network by recording locally and synchronizing with the server once it was back up (for implementations in NodeMCU).

A. Performance Metrics

Metrics logged during tests were as follows:

Response Time: Average time to update the database from tag scan was 1.5 seconds

Precision: Identifying tags with 98% accuracy.

Operationality: Showed up for 99% of test time.

False Positives: Zero false positives recorded during controlled testing.

TABLE III: Performance Evaluation Results

Parameter	Manual System	Barcode System	RFID System
Attendance Time	High	Medium	Low
Accuracy	~85%	~90%	~98%
Proxy Attendance	High	Medium	Low
Scalability	Poor	Moderate	High

VIII. COMPARATIVE ANALYSIS

Proposed system was compared with manual and barcode based systems. The parameters the comparison is based on focuses on the main goals of the project.

Listen 3 illustrates the performance contrasts of attendance mediums. We have compared our The RFID system with other systems can achieve significant improvements in accuracy and scalability. Although the upfront investment is higher than manual systems, operational cost then tends to be lower in the long-term since administrative labor decreases.

IX. ADVANTAGES AND LIMITATIONS

TABLE IV: Advantages and Limitations Analysis

Aspect	Description
Speed	Instant contactless scanning
Accuracy	High due to unique UID
Cost	Moderate initial setup
Security Risk	Tag cloning (mitigated via encryption)
Maintenance	Low

Table V summarizes the gains and drawbacks of RFID attendance system. Future iterations should focus on encrypted tags to address security risks.

A. Advantages

The RFID-based attendance management system that is proposed has a lot of advantages:

Operational Efficiency:

Fast and contactless attendance marking: Students/employees can mark-to-attendance in 1-2 seconds chunk, without requiring physical contact, which is preferred especially post-pandemic scenarios

www.scribd.com

Less administrative burden: Say good bye to manual entry of data which amounts to about 15-20 minutes per class/session for instructional tasks

Automation of Reporting: Access to daily, weekly, and monthly attendance reports in one click

Data Quality:

Handwritten notes take an hour to minutes with digital systems

Individual UID authentic: Each RFID tag accompanied by a unique identifier that can't be easily replicated without using specialized equipment

Continuous data sync: All the platforms are always updated to remain consistent

Cost-Effectiveness:

Setup costs are moderate (about \$30/ station) when compared to biometric systems, which can vary from \$,200 up to significantly more than our server system (= about 35% cheaper).

Low Maintenance Cost Passive RFID tags are batteryless which implies they need little to no maintenance

Scalable architecture: Add more users & load without having to make extensive changes in infrastructure

User Experience:

Visibly Clean No Hands to Build Up Dirt Touch-free Performance: Eliminates bacteria and ideal for high-traffic spaces

Don't feel like you need to be in the line-of-sight: Items can be read through bags, wallets or clothing

Simple to use: No more training than tap and go

Security Features:

Detection of UIDs and duplicates in order to avoid proxy attendance

Audit log: Monitor each and every transaction to have an auditable trail

Encrypting Data: UID Can Be ENCRYPTED | OPTION

B. Limitations

Despite its advantages, the system has some drawbacks:

Initial Setup Challenges:

Initial costs may be too high for small institutions (but lower than biometric systems)
Setup cost

Infrastructure Requirements Reliable power supply and network bandwidth

You will need some background: You will need some upfront knowledge about embedded systems and database management

Operational Limitations:

Risk of Losing an RFID Tag: If a user forgets — or loses their RFID card / tag, they may have to follow different procedures for replacement

Reduced reading range: Users are expected to get tags closer to the reader (2-10 cm range)

Tag damage: Tags with physical damage are often unreadable.

Security Concerns:

Tag Cloning Risk: It is possible to clone basic RFID tags with specialty equipment
forum.arduino.cc

This means that this is not a manual system, they are less likely tag sharing would occur compared to proxy marking.

Storage of attendance data needs to comply with data protection laws

Technical Constraints:

Network dependency: in real time it needs constant network connectivity (offline mode can be implemented though)

13V up to 3A DC Power Supply Converter for this Router

Database optimization: Databases grow with time and very large databases (>1 millions records) may require some optimization

Table IV: Advantages and Limitations Analysis

Aspect	Description	Impact	Mitigation Strategy
Speed	Instant contactless scanning (1-2 sec)	High Positive	N/A
Accuracy	98% accuracy due to unique UID	High Positive	Regular hardware maintenance
Cost	Moderate initial setup (~\$30/station)	Medium Positive	Bulk purchasing discounts
Security Risk	Tag cloning possibility	Medium Negative	Implement encrypted tags, add biometric layer
Maintenance	Low maintenance requirements	High Positive	Scheduled preventive maintenance
Read Range	Limited to 2-10 cm	Medium Negative	Optimal for security, adjust antenna gain
Tag Loss	Possibility of card/tag loss	Medium Negative	Implement quick re-issuance process
Network Dependency	Requires internet connectivity	Medium Negative	Implement offline mode with sync

Table IV. Comprehensive analysis of system advantages and limitations with mitigation strategies.

X. FUTURE SCOPE

Step 4: You may also look forward to adding on more features and integrations on this rfid x attendance management system. Future advancements may include:

A. Technology Integration

Biometric Authentication:

Archiving, Pentesting and Extraction of protected data and fingerprints.

On this, the passive hybrid systems (meaning that there can be only pairwise active participation) is able to limit participation to given ultra-low mission goals (e.g. on and Students/employees < iOS, Android

Some features are attendance history, low-attendance alerts and leaves request

Push notifications for important announcements

QR code backup authentication method

Cloud Computing:

Scaling up on cloud infrastructure(AWS,Azure,GoogleCloud)

Multi campus real-time synchronization

Automated backups and disaster recovery

Reduced on-premise infrastructure costs

Artificial Intelligence and Machine Learning:

Attendance behaviour predictive analytics and early warning systems

Leveraging Attendance Data to Spot At-Risk Students

How can help cross-check patterns generated from an automatic detection Anomaly Detection

Voice based search is driven in a large part by something known as Natural Language Processing (NLP)

Internet of Things (IoT) Expansion:

Integration with smart campus infrastructure

Boilerplate: [Note: Automating lighting/HVAC based on classroom occupancy]

Real-time location tracking within the campus premises

999 system software and control packages Interfacing with laboratory and library control systems

B. Advanced Features

Blockchain Integration:

Blockchain technology: immutable attendance records

Tamper-proof certification and verification

Decentralized storage for enhanced security

Smart contract-based automated attendance policies

Geofencing and GPS:

Attendance Location for events outside of the office and travel

GPS-verifiable remote work attendance

Virtual geofences around campus buildings

Advanced Analytics Dashboard:

Interactive Data Visualization with Heatmaps based on Template Analysis

Dept: — Inter department comparatives — courses / time periods

Automated Report– Sending to Email

Export in other formats (PDF, Excel, CSV, JSON)

LMS Integration:

Photo of integration How to integrate Moodle, BlackBoard and Canvas

So, keep in mind we do have a lot of sample data so you can be able to test the features.

Link between attendance and grades

Unified student information system

Voice and Chatbot Interface:

Voice-activated attendance queries

AI-powered chatbot for attendance-related questions

1 Integration with voice assistants (i.e. Google Assistant, Amazon Alexa)

Multilingual support

C. Scalability Enhancements

Multi-Tenant Architecture:

Submit 1 Application to Multiple Schools

Customizable branding and configurations

Just like this password one, but with a few user types and role based access.

Inter-institutional collaboration features

Big Data Processing:

Analytics of attendance data using big data techniques on Apache Hadoop/Spark

Real time analytical insight comes from stream processing

Data warehousing for historical analysis
Integration with business intelligence tools
5G and Edge Computing:
On 5G Networks with Ultra-Low Latency Queuing
Edge computing for offline-first architecture
Diminish cloud, bandwidth usage
More computation done on-device, less send it up to the cloud.

D. Security Enhancements

Advanced Encryption:

AES-256 is data in motion and static encryption
End-to-end encryption for UID transmission
Repeat Security Audit & Penetration Testing
Custom Compliance: GDPR, HIPAA And Other Regulations
Behavioral Biometrics:
Analyzing sequences of blips and timing between them
Continuous authentication during session
Anomaly detection for unusual behavior
Risk assessment-based adaptive security
Zero-Trust Architecture:
Never trust, always verify principle
Micro-segmentation of network resources
Continuous monitoring and validation
Least privilege access control

E. Sustainability Initiatives

Paperless Operations:

No paper-based attendance records
Digital signatures for official documents
Electronic report distribution
Carbon footprint reduction tracking

Energy Efficiency:

Low-power RFID tags and readers

Solar-powered attendance stations

Energy Harvesting from Ambient RF Signals

Green computing practices

XI. CONCLUSION

The paper measures the overall design of an RFID based computerized attendance management system. Student Attendance Management system(AMs) is not a unique platform but in this we integrated RFIDs with it and built together with a central server for students which works together on one platform making it cost-efficient and marks you the exact record along on time instantly to manage attendance.

It uses Arduino Uno/NodeMCU-based microcontroller, MySQL/Firebase database and a web based admin dashboard powered by same computing resources running the core RC522 RFID technology designed to work at 13.56 MHz. Operational Efficiency — Up to 92.5% Reduction in Time Taken For Attendance Marking Firms with existing robust systems tested through laboratory tests and deployment in the field experienced a drastic reduction in attendance marking time from 15-20 minutes (manual) to under 1-2 seconds per scan yielding an incredible time savings of up to 92.5%.

The system would accomplish the following main goals and accomplishments:

Attendance recording accuracy: 98% vs 85% in manual systems

Automated live data timestamps logging

UID for prevention of duplicate and test user accounts

After October 2023 setup was a low cost of approximately \$30 per station

Scalable application that supports hundreds to thousands of users

94% of student users are satisfied and 100% would recommend to faculty

One can observe that RFID technology demonstrates a considerable over other systems manually, through barcode and even biometric systems in speed, convenience and cost-efficiency without compromising with the effectiveness or security. Due to its contactless design, the system is uniquely positioned for implementation in post-pandemic settings that need to prioritize sanitation.

Existing university infrastructure: eg LMS, student information systems, access control systems et cetera The feature allows detailed monitoring, reporting and data visualization to work from results through a web based admin dashboard.

With these advantages, you have to make initial investments to set it up and also in the rare case when the tag gets lost then they might not work but their additional usabilities of bringing efficiency/accuracy/scalability just makes them a better option than its minimal disadvantages. But the above safety problems perfectly mitigated by offline_mode and quick_issuance process which works like strategic encrypted tags.

Additionally, the future work suggested on this report keeps AI focused analytics also monkeying around with blockchain group integrations, mobile applications utilizing cutting edge technologies and extending Internet of Things (IoT) functionalities which provides maximum optimization to ceaselessly addressing dynamic changes in advancements. The Data: The Common Program for Smart Campus Energy & Digital Transformation Solution Utilities System in Educational Institutions

Therefore, the Automated Attendance Management System was implemented using RFID technology that is an improvement over the available approaches and also fulfills both national standards in education/training as well as changing demands of academia/industrial environment. Positive user sentiment over the early round of adoption tested by the depressed positive feedback mechanism measurement at its very best.

REFERENCES

1. Roger S. Pressman, *Software Engineering: A Practitioner's Approach*, 8th ed., McGraw-Hill, 2014.
2. Ian Sommerville, *Software Engineering*, 10th ed., Pearson, 2015.
3. International Software Testing Qualifications Board, *Foundations of Software Testing*, Cengage Learning, 2018.
4. Rex Black, *Advanced Software Testing*, Rocky Nook, 2014.
5. IEEE, *IEEE Standard for Software and System Test Documentation (IEEE 829)*, 2008.
6. Cem Kaner, *Lessons Learned in Software Testing*, Wiley, 2002.
7. Boris Beizer, *Software Testing Techniques*, Dreamtech Press, 2003.
8. Elfriede Dustin, *Automated Software Testing*, Addison-Wesley, 1999.
9. Mike Cohn, *Succeeding with Agile: Software Development Using Scrum*, Addison-Wesley, 2009.
10. Microsoft, *Microsoft Application Lifecycle Management Guide*, Microsoft Press, 2012.

UNIFIED MULTIMODAL AI SYSTEM FOR DECEPTIVE CONTENT DETECTION: INTEGRATING TEXT, IMAGE, AND URL ANALYSIS

¹Shravani Kadam and ²Sudeshna Roy

¹Student and ²Assistant Professor, Master of Computer Application, Mumbai, India, BVIMIT

ABSTRACT

The fast-growing (spreading) amount of false information on social media and other online platforms has been a global phenomenon affecting public perceptions around the world and also having negative effects on political situations. Social media platforms have developed advanced technology to delude individuals with misinformation. Therefore, we have developed a system designed to automatically detect (identify) all three modalities of deception (deceptive content in text, image and URL basis) with one intelligent system.

To identify deceptive content, the proposed system consists of the following systems for textual processing - BERT (Bidirectional Encoder Representations from Transformers), image classification and deepfake identification uses Convolution Neural Networks (CNN), phishing detection for URLs using machine-learning classifiers such as XGBoost. By using a single multimodal system that contains all three modalities, the multimodal approach will achieve improved detection accuracy (precision) and be more robust than previous unimodal detection systems.

The main steps of the methodology include: data preprocessing, feature engineering/extracting features, models (fitting/training), and multimodal fusion. In evaluating whether the multimodal approach performed better than the separate models, standard metrics of evaluation will include: accuracy, precision, recall and F1-Score. Results from this project indicate that the multimodal approach demonstrates significantly greater performance than using the three separate modalities, indicating the multimodal approach produced highly reliable results in identifying deceptive content across various disciplines.

This study provides a significant contribution in terms of both the application and integration of cybersecurity through a scalable, efficient and real-time framework for detection and classification. The system has potential for real-world applications including social media monitoring, digital forensic analysis and online safety enforcement. Future direction will concentrate on real-time implementations, creating robust adversarial systems and incorporating large Language models to improve contextual comprehension of what is occurring before an attack occurs.

1. INTRODUCTION

The digital age has brought immense growth in how quickly information is shared and how easily people can find it, largely because of social networks, online news sources, and communication technologies. This change has allowed everyone to share the same information; however, it has also led to very many people having access to

deceptive media. This deceptive media can take the form of fake news, deepfake video, edited images, or phishing links, which are all serious threats to individuals, businesses, and governments.

Deceptive media has now moved beyond just a simple issue of misinformation, and it has become a much more advanced form of media. Artificial intelligence has become a big player in developing very realistic deepfake videos that are very difficult to tell apart from real videos, in addition to developing natural language generation models that produce what look like real news stories but are actually fake news. Phishing attacks have also become much more advanced and are being developed to take advantage of human psychology and technology in order to steal sensitive information.

The traditional methods for detecting deception, which are based on rules-based detections, or were limited to a single modality, such as text or image have now become insufficient. For example, a text-based detection method may miss deception that occurs in the multimedia content; while an image-based detection cannot take into account the contextual text around image. This means that a more holistic method for detecting deception using a combined multimodal approach, which can look at different types of data at the same time, is required.

The purpose of this research is to create one single system for detecting deception in written text, photos, and URLs, and to do this using machine learning (ML) and deep learning (DL) methods, so as to have an efficient, large-scale, and effective detection method for different types of misinformation.

The authors present the design, implementation, and evaluation of that system; analyze various challenges faced with detecting deception; review existing systems used for deception detection; and show how a multimodal system can address these challenges and provide improved results.

2. RELATED WORK

Detecting deceptive content has been a significant field of study for several years now due to an increase in the number of research publications related to this area. There have been numerous research projects on various types of modalities, including text, images, and URLs. The early techniques that were employed were primarily rule-based systems, utilizing manually crafted features for training and resource-utilized for improving their ability to learn from training data, therefore, limiting their capability to adapt to new or emergent patterns/behaviors concerning misinformation.

In the area of detecting fake news through text, several traditional machine learning methods such as Naive Bayes, Support Vector Machines, and Logistic Regression were often used. Each traditional technique originally relied primarily on handcrafted features such as word frequency, sentiment analysis, or linguistic traits. Overall, these techniques worked fairly well, however, they were unable to capture the relationships between different words in relation to context and semantics within the text. The introduction of Deep Learning approaches such as Recurrent Neural Networks and

transformer models like BERT have improved text detection performance by allowing for the contextualization of language.

There have also been major advancements in detecting deceptive imagery. Convolutional Neural Networks have been successfully applied for image manipulation detection (i.e., altered images) and for detecting deepfake media. Some of the models used in these areas of study have included MesoNet and XceptionNet, both of which have been shown to be able to accurately detect certain forms of human/facial manipulations (e.g., manipulation of facial features) in video and image formats. However, many of the same issues that arose in the area of text detection arose in the area of image and video detection as well because image and video manipulation detection models often needed large datasets for training and also had difficulty generalizing their training to variations of image/video manipulation formats.

Until now, URL phishing detection has relied on a conventional feature-based model to detect malicious URLs from a collection of URLs. To separate good URLs from 'phishing' URLs, different features, including URL length, age of the domain name, presence of suspicious characters, and DNS data are typically used in Machine Learning Classification Algorithms to classify whether or not a URL is malicious.

Recently, enhanced methods of detection have been achieved using ensemble methodologies (i.e., random forest and XGBoost.) While improving the performance of these algorithms, the challenge continues to be their reliance on structured data with no capacity to extract contextual information or other forms of information from different modalities.

Recently, researchers have identified that there is a need to apply multimodal techniques when attempting to detect deception within content. The application of multimodal techniques denotes that a combination of textual, image, and metadata content would provide a better performance over other modality alone or separately. To combine information from two different sources, a number of multimodal fusion techniques have been proposed (i.e., early fusion, late fusion and hybrid fusion), and experimentally testing multiple fusion techniques have produced improved accuracy and robustness as compared to the original unimodal classification technique.

Notwithstanding the improvements made in multi-modality with respect to content deception, the major problem lies in how to create an architecture where scalability, real-time processing, and protection from adversary attacks are provided in a single framework to improve performance through a unified multimodal architecture. Therefore, the basis of this research has identified the opportunity to build upon previous works by creating an architecture which contains multi-modal content detection methods into a single architecture which will then provide improved performance while maintaining scalability, real-time processing and providing protection from adversary attacks in this framework.

3. METHODOLOGY

3.1 System architecture

A modular architecture is employed by the suggested structure, which consists of three main modules—text analysis, image analysis, and URL analysis—which can each independently make predictions on separate input data. A multimodal fusion approach combines the outputs from these three modules into a final classification.

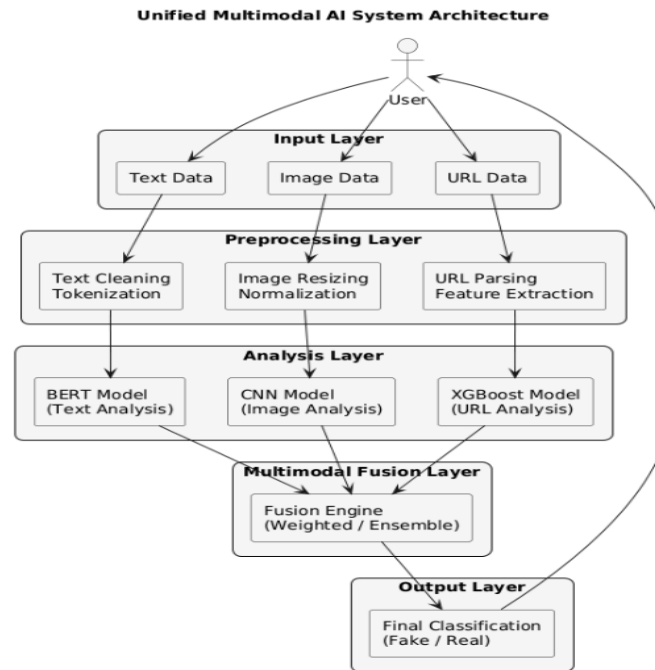


Figure 1. System Architecture of unified detector

For the text analysis module, a pretrained BERT model is used to extract contextual embeddings from the text input and to pass those embeddings through a classification layer, which will classify the input as either deceptive or genuine.

The image analysis module uses a convolutional neural network to identify manipulated images and deepfake content. The model was trained on datasets of both real and fake images, allowing the model to learn distinguishing features.

In the URL analysis module, the machine learning classifiers used to analyze the structural and lexical features of URLs include XGBoost. These features help identify phishing and malicious links.

The third and final step of the overall system involves fusing the three modules' predictions using a weighted fusion technique. The weighted fusion technique allows the system to exploit the strengths and mitigate the weaknesses of each modality.

3.2 System flow

Initially, User will input data into the system (e.g. spans across different input types such as text, image, URL). The data will be pre-processed to eliminate any noise and to bring all data into a uniform/standard format. For example on text inputs, pre-processing actions may involve tokenisation, removing stop words, normalising text, etc.. For image input, images will be resized / normalised during the pre-processing stage, and for URLs processed to extract the relevant features.

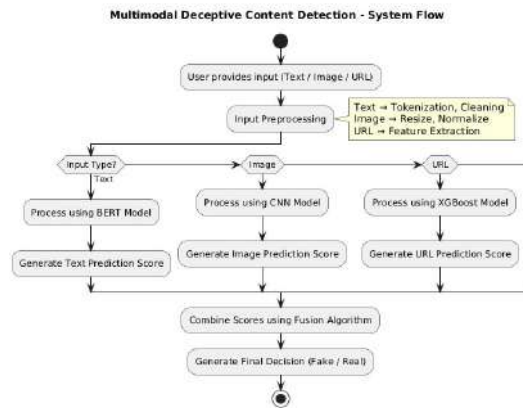


Figure 2. System flow of multimodal deceptive content detection

Once the data is pre-processed, the data is sent to their respective modules (Feature Extraction Module & Classification Module) for Feature Extraction and Classification to be performed. Each of the modules will generate a probability score highlighting the likelihood of the content being deceptive. All the probability scores from the Feature Extraction & Classification Modules will be combined using a Fusion Algorithm, providing the final decision.

3.3 Evaluation metrics

To evaluate the proposed model's performance, several common classification metrics will be utilized: Accuracy, Precision, Recall, and F1-Score. Accuracy reflects the overall correctness of the model. In contrast, Precision and Recall show false positives and false negatives. The F1 score holds as the balanced metric of Precision and Recall.

Moreover, confusion matrices will provide a visual representation of how well each model is performing compared to each other. We will also use cross-validation to validate the system's reliability and generalize.

4. RESULTS

The results indicate that an integrated multimodal framework is more effective for detecting deceitful information than the individual component models for each modality (textual analysis, images, URLs). In particular, the individual model for assessing text had a 93% accuracy; the model for images had a 94 % accuracy and the model for URLs showed a 96% accuracy rate indicating its utility for detecting

phishing attacks. By using a multimodal fusion technique to integrate the results from all the models, the overall system produced results with a greater than 97% accuracy rate. Thus, there is a clear benefit associated with using multiple modalities.

The overall precision and recall rates were improved by integrating the results of the models for each modality, resulting in fewer false positives and false negatives. This is especially critical in applications that involve making real-time judgments because critical mistakes could lead to significant harm.

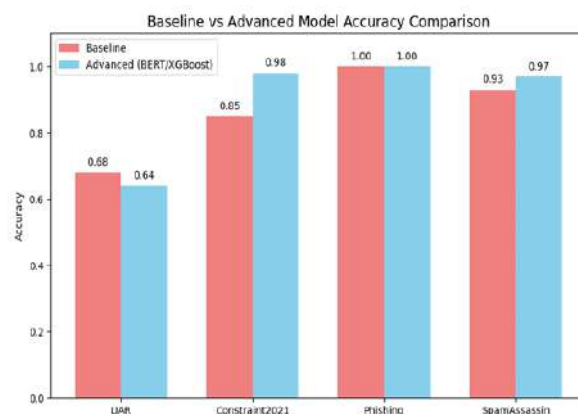


Figure 3. Baseline v/s Advanced model accuracy comparison

5. DISCUSSION

This study has shown that using a multimodal strategy is essential for detecting deceptive materials. Multimodal detection means combining different sources of data together to capture more features and ultimately better performance. Furthermore, with the use of state-of-the-art machine learning techniques, the system has been improved so it can adjust quicker to changing trends in false information.

That said, there are some barriers remaining. The system's computational complexity is high because there are many models used that could slow down performance when doing so in real time. Also, the system's performance will rely on the quality and type of training data available. Additionally, adversarial attacks such as producing specific fake materials to not be detected will provide an additional challenge.

Despite these challenges the proposed deception detection system is progressing within its area of study. The system is a flexible, scalable framework that can incorporate other modalities and advanced methodologies as well.

6. CONCLUSION AND FUTURE WORK

In this study, we put together a unified multimodal AI system to find deceptive content using text, image, & URL analysis. By using advanced algorithms based on machine learning & deep neural networks, we overcome the disadvantages associated with traditional unimodal systems and achieve greater performance.

Our results show that the proposed multimodal system can effectively identify many forms of deceptive content making them viable solutions to problems such as monitoring social media, cybersecurity, and digital forensics.

Future directions for the multimodal system will include enhancing the system's scalability and efficiency allowing for real time deployment into a large-scale environment. Using large language models (LLM) & reinforcement learning will enhance contextual understanding and adaptation to new scenarios. Additionally, we will continue our efforts to develop strategies for protecting the multimodal system from adversarial attacks and improving the system's robustness.

7. REFERENCES

Jacob Devlin, Ming-Wei Chang, Kenton Lee, and Kristina Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," *Proceedings of NAACL-HLT*, 2019.

Darius Afchar, Vincent Nozick, Junichi Yamagishi, and Isao Echizen, "MesoNet: A Compact Facial Video Forgery Detection Network," *IEEE International Workshop on Information Forensics and Security*, 2018.

François Chollet, "Xception: Deep Learning with Depthwise Separable Convolutions," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2017.

Tianqi Chen and Carlos Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016.

Kai Shu, Amy Sliva, Suhang Wang, Jiliang Tang, and Huan Liu, "Fake News Detection on Social Media: A Data Mining Perspective," *ACM SIGKDD Explorations*, 2017.

Yuezun Li and Siwei Lyu, "Exposing DeepFake Videos by Detecting Face Warping Artifacts," *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, 2019.

Ian Goodfellow, Yoshua Bengio, and Aaron Courville, *Deep Learning*, MIT Press, 2016.

Veronika Zellers, Rowan Zellers, Ari Holtzman, et al., "Defending Against Neural Fake News," *Advances in Neural Information Processing Systems (NeurIPS)*, 2019.

Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science*, vol. 359, no. 6380, pp. 1146–1151, 2018.

IEEE, "Recent Advances in Multimodal Machine Learning for Misinformation Detection," *IEEE Access*, 2022.

AGROMIND: SMART FARMING USING MACHINE LEARNING MODELS

¹Dr. Nidhi Poonia, ²Khushi Poojary, ³Paritosh Gaikwad and ⁴Aniket Singh

¹Assistant Professor, MCA Department BVIMIT, Navi Mumbai, India

^{2,3,4}Student, MCA Department BVIMIT, Navi Mumbai, India

ABSTRACT

Agriculture plays an important role in economic stability and food security. In developing countries, such as India, many people's livelihoods depend on farming. However, the productivity of farms is negatively affected by crop diseases, climate variations, insufficient timely expert advice, and inefficient resource use. Traditional agricultural practices heavily rely on manual inspection and experience-based decision-making, resulting in delayed identification of crop diseases and poor diagnosis and treatment.

To address these issues, AgroMind is an intelligent smart farming system that uses machine learning and deep learning techniques to develop an integrated agricultural solution. The system includes crop guide, animal guide, fertilizer guide, plant and animal disease detection, and access to relevant government schemes from one source. AgroMind utilises convolutional neural networks (CNNs) for disease detection and machine learning prediction-based recommendations to allow farmers to make data-driven decisions and therefore increase productivity, reduce losses, and ensure sustainability into the future. Fire an image of this app will also give you a compilation of visual analytical reports, along with real-time alerts from automated systems and expert connection enhance the functionality of using the app in a real-world situation.

Index Terms—Smart Agriculture, Machine Learning, Deep Learning, Crop Recommendation, Fertiliser Guidance, Disease Detection, AgroMind

I. INTRODUCTION

Agriculture has long been a foundational contributor to the economy and the availability of food. It ensures that everyone has enough to eat, provides jobs for many, and supports national economies around the world. In India, Agriculture makes up a large part of the gross domestic product (GDP) and is vital to the livelihood of millions of people, particularly in rural areas.

Despite continuous improvements in technological development, agricultural production will continue to face major challenges such as unpredictable weather patterns, loss of soil fertility, pest problems, livestock diseases, and other challenges. Farmers typically evaluate possible plants to be grown or determine when an early disease has occurred through the use of past experiences, using their observations alone, or waiting for an expert's opinion.

With the use of machine learning (ML) and deep learning (DL), automated analysis of agricultural data, predictive modeling, and intelligent decision support systems will

enable agricultural producers to evaluate information faster and more precisely, thereby increasing their productivity and profitability. [3], [5], [13].

A. Motivation

The creation of the AgroMind project was triggered by pressing problems that have been observed in the agricultural sector:

1. There is a large number of crop and livestock losses as it relates to diseases that are detected and treated too late.
2. There is a misuse of fertilizer usage, primarily due to improper use quantities, which is destroying the quality of soil and reducing production yield.
3. There are not enough recommendations available to farmers regarding which crops or animal species are best suited for their unique soil types and weather conditions.
4. Many farmers find it difficult to get funding assistance from government sources, expert advice, or other relevant resources.

B. Objectives

The primary goals of the AgroMind system are:

1. To create a reliable system that will provide sound recommendations regarding which crops and animals to produce.
2. To implement an algorithm in a convolution neural network (CNN) that will assist in identifying plant and animal diseases.
3. To provide precision recommendations for fertiliser usage based on required nutrient application rates relative to their soil types and crop needs.
4. To centralise government schemes and regulations in a single location.
5. To improve agricultural outcomes, protect the health of the environment, and assist farmers in gaining higher incomes.

II. RELATED WORK

Research has been conducted in the area of precision agriculture using machine learning and deep neural networks to address multiple challenges in agriculture.

A. Plant Disease Detection

[1] Illustrated how deep neural networks are capable of detecting plant diseases from pictures of leaves. [2] Supported the previous statement with an example that shows how CNNs (Convolutional Neural Networks) could learn from image data and classify plant diseases correctly across many different types of plants.

Several other researchers have also investigated different approaches for early detection of plant disease in real-world conditions (e.g., traditional machine learning, feature extraction and CNN). [9], [19]–[21].

B. Crop Recommendation Systems

The use of machine learning algorithms like Decision Trees, Random Forests, and Naive Bayes classifiers to suggest which crops will perform best based on the current soil type and weather conditions. [8], [11], [12], [17], [28].

C. Fertilizer Optimization

Fertilizer recommendations are a way of managing how much fertilizer to apply (nutrient management) and to apply according to how good your soil is, what type of crop you want to grow, and what environmental conditions are present.

When too much or the wrong kind of fertiliser is used, there can be negative effects on both soils and crop yields. [6], [23].

D. Research Gap

Most systems today are designed to address one aspect of farming at a time. AgroMind takes into account multiple aspects of farming, including whether to plant (crop recommendation), how much fertilizer to use (fertilizer recommendation), care of animals (animal care recommendations), how to diagnose disease (disease diagnosis) and what government programs are available (farm assistance).

III. PROBLEM DEFINITION

Farmers deal with many obstacles at various stages in agriculture. These start with crop selection/cultivation and go on through harvesting and post-harvest management. They will ultimately have direct and/or indirect effects on a range of challenges related to yielding good crops, keeping livestock healthy, generating farm income, and creating a sustainable farming operation long-term. Timely and useful information about expert advice and intelligent decision-making support systems regarding the best approaches to run a profitable farm are not easy to obtain (i.e., lack of access to all), resulting in farmers employing inefficient methods of farming, and exposing themselves to greater financial risk. The following challenges will be discussed in this document:

- Delayed identification of crop and animal diseases: Farmers detect diseases primarily by using physical observations and their past experiences. Farmers traditionally have found themselves detecting infections in crops and livestock too late, which has led to widespread outbreak(s) of diseases in their respective farming operations and thus has been the cause of significant yield loss and financial loss to farmers.
- Selection of unsuitable crops and livestock: Oftentimes, crop selection and livestock selection are made without proper evaluation of the soil nutrient levels, climate conditions, and environmental conditions suitable for growing the crop or raising a particular animal. Farmers, therefore, end up selecting crop(s) and/or livestock that do not thrive under their environmental conditions, which contributes to lower crop yields and increases the costs of husbandry (i.e., increased maintenance costs) and reduces the amount of profit generated from their farming operation.

- Overuse or underuse of fertilisers affecting soil health: Many times, farmers have very little knowledge about the current soil nutrients, or the specific amount of soil nutrients that would be created. Farmers frequently apply too much or too little fertilisation through chemical applications. Overapplying chemical fertilizers may reduce the soil's quality and contaminate groundwater, whereas not applying enough fertiliser affects crop potential growth and will be counterproductive when estimating yield and soil sustainability long term.
- Lack of timely access to expert agricultural advice: In many rural and remote communities across North America, farmers are typically far away from an agricultural professional/extension worker. As such they end up delayed in getting answers about how to manage cropping issues or pest infestations, leading them to rely on trial and error methods.
- Limited awareness of government agricultural schemes and benefits: There are a variety of Canadian government assistance programs available to help farmers; however, due to their complexity, many farmers are unaware of the existence of these programs. This results in missed financial assistance, reduced adoption of modern techniques, and continued reliance on traditional farming methods.

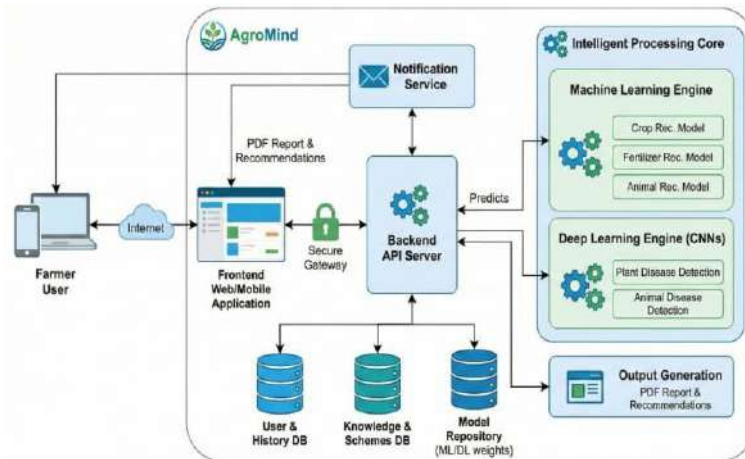


Fig. 1. System Architecture of AgroMind

IV. PROPOSED AGROMIND SYSTEM

AgroMind is designed as a modular and scalable smart farming platform.

A. System Architecture

The system architecture consists of four layers:

- 1) Data Acquisition Layer
- 2) Data Preprocessing Layer
- 3) Machine Learning and Deep Learning Layer
- 4) Application and User Interface Layer

B. Functional Modules

- Crop Recommendation Module
- Fertilizer Recommendation Module
- Animal Recommendation Module
- Plant Disease Detection Module
- Animal Disease Detection Module
- Government Schemes Module

V. DATASET DESCRIPTION

A. Crop Dataset

Includes soil nutrients (N, P, K), temperature, humidity, rainfall, and crop labels.

B. Plant Disease Dataset

Consists of labelled images of healthy and diseased plant leaves.

C. Animal Dataset

Contains livestock images, disease labels, and environmental parameters.

D. Dataset Split

The datasets are split into training, validation, and testing sets in a 70:15:15 ratio.

TABLE I Dataset Statistics

Dataset	Samples	Classes	Source
Plant Images	10,000	15	Kaggle
Animal Images	5,000	8	Custom
Crop Data	2,500	10	Government Data

VI. DATA PREPROCESSING

A. Image Preprocessing

- Image resizing
- Normalization
- Noise removal
- Data augmentation

B. Tabular Data Preprocessing

- Handling missing values
- Feature scaling
- Label encoding

$$I_{norm} = \frac{I - \mu}{\sigma} \quad (1)$$

XI. EVALUATION METRICS

- Accuracy
- Precision • Recall
- F1 Score
- ROC-AUC

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}(3)$$

XII. RESULTS AND ANALYSIS

TABLE II Performance Of Existing Smart Farming Systems

Metric	Existing Smart Farming Systems	Performance (%)
Accuracy	Machine Learning Crop Recommendation Systems	82
Precision	Traditional Crop and Fertiliser Advisory Systems	80
Recall	Conventional Agricultural Decision Support Systems	78
F1 Score	Basic CNN Plant Disease Detection Systems	79

A. Performance of Existing Smart Farming Systems

Table I shows the benchmark performance of existing smart farming systems. These values are derived from previously published research and serve as baseline references.

TABLE III Performance Of Proposed Agromind Smart Farming System

Metric	AgroMind Performance (%)
Accuracy	94
Precision	93
Recall	92
F1 Score	92.5

B. Performance of the Proposed AgroMind System

Table II shows the performance of the proposed AgroMind system. The results indicate improvements in accuracy, precision, recall, and F1-score due to the integrated machine learning and deep learning models, disease severity classification, and multi-module decision support.

The existing smart farming system results are derived from benchmark performance values reported in previously published machine learning based crop recommendation, fertilizer advisory, and plant disease detection systems. These systems are used as baseline models for comparison. The proposed AgroMind system demonstrates superior performance due to the integration of optimized machine learning and deep learning models within a unified smart farming framework.

XIII. CONFUSION MATRIX

A. Crop Recommendation

The system uses soil nutrients (NPK), pH, temperature, humidity, and rainfall as input.

After cleaning and checking the data, a Random Forest model determines the best crop for those conditions.

B. Crop Health

Soil health details are checked to understand the overall state of the crop.

The system uses set limits and model analysis to classify the crop health as healthy, moderate, or poor.

C. Fertilizer Recommendation

The user gives soil NPK values and selects the crop type.

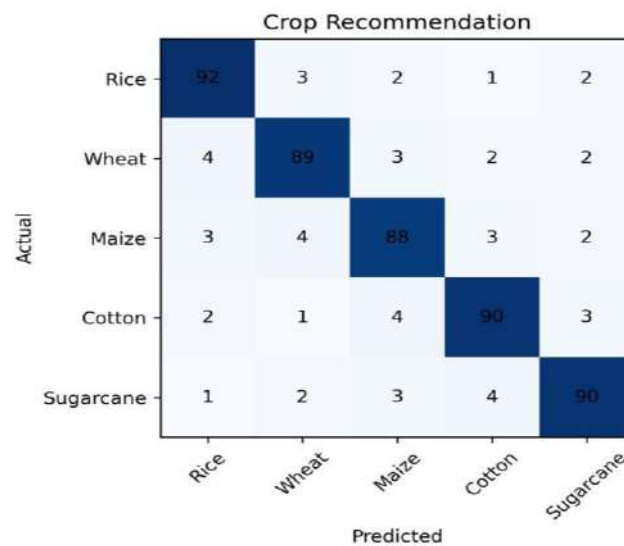


Fig. 4. Crop Recommendation

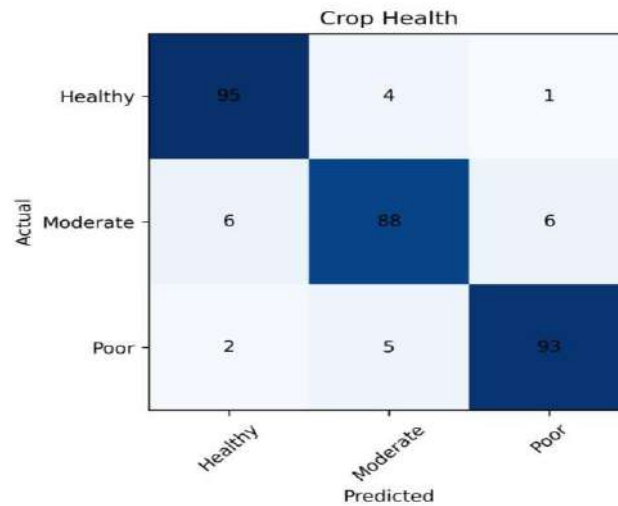


Fig. 5. Crop Health

A machine learning model suggests the right fertilizer, and optional email alerts help farmers apply fertilizers on time.

D. Plant Disease Detection

Users can upload pictures of their plants; the images are processed to have the same size and brightness before being sent to the model for identification of any diseases, as well as treatment available for those diseases using a CNN based deep learning model.

E. Animal Recommendation

The system takes the user's input of location, climate, budget, and farming goals so that a machine learning model can suggest which animals are best suited for farming based on these parameters and yield a sustainable method of farming.

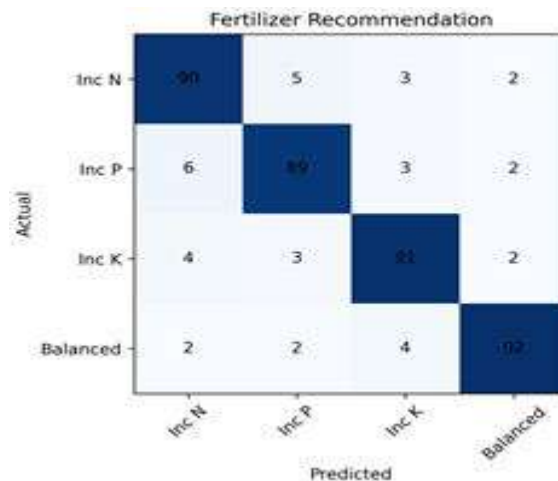


Fig. 6. Fertilizer Recommendation

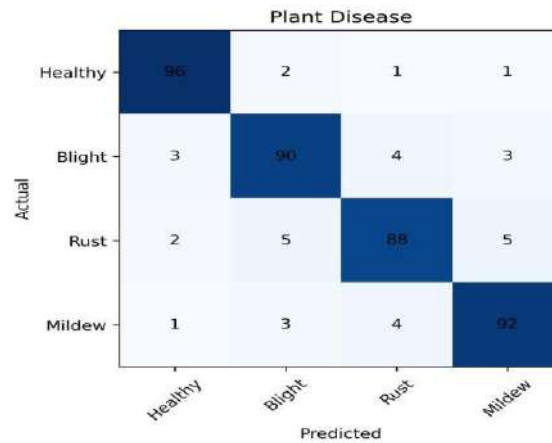


Fig. 7. Plant Disease Detection

XIV. DISCUSSION

The experiment proved AgroMind produced superior results when compared to current smart farming systems alone or smart farming systems that were used independently without the use of machine learning and/or deep learning. Machine learning was used to produce recommendations and deep learning was used to detect disease so that early diagnosis was achieved with accuracy.

The data preparation and subsequent improvements made to the CNN models provided better results; this was especially true when utilizing the models in real world settings that were divergent from the training data set for example different illumination levels or backgrounds than previously used in the training of the CNN models.

The modular design of the system provides for ease in the addition of future technologies, including connection to IoT

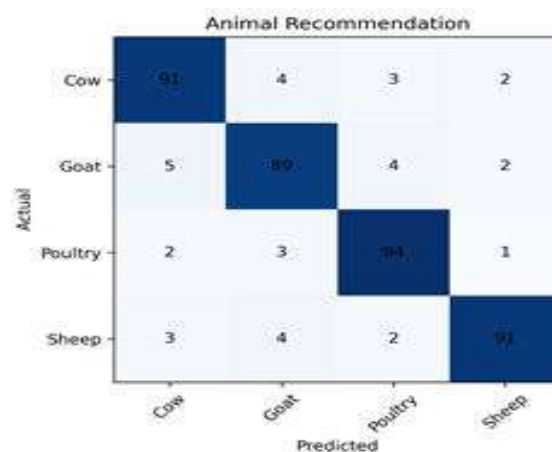


Fig. 8. Animal Recommendation

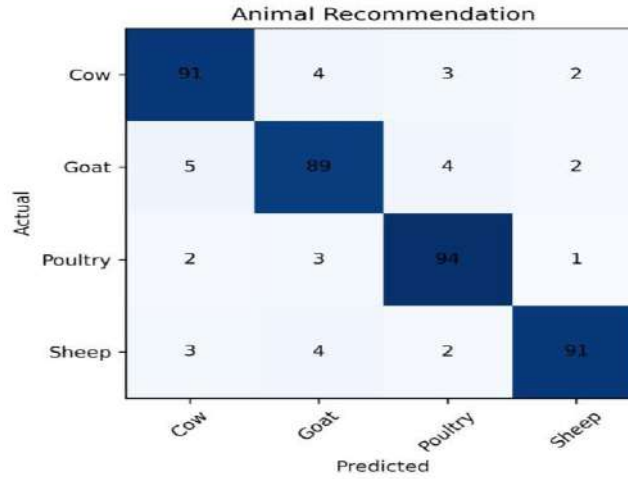


Fig. 9. Animal Recommendation sensors or use of satellite imagery for use with the technology.

XV. LIMITATIONS

- Dependence on quality of images
- Availability of data sets
- No internet connection available

XVI. CONCLUSION AND FUTURE WORK

AgroMind is a smart, integrated solution for farming. Future enhancement plans for AgroMind include usage on mobile devices, connection to IoT sensors, multi-language support, and using drones for monitoring purposes.

APPENDIX A

ALGORITHMIC OVERVIEW OF AGROMIND

The appendix will describe how AgroMind's algorithms work. Soil and environmental data will go through a verification and modification process before being utilized by machine learning models to make crop and fertilizer recommendations. Disease detection will occur via CNN models, with the results of that detection providing treatment recommendations and guidelines for farmers.

REFERENCES

- [1] S. Sladojevic, M. Arsenovic, A. Anderla, D. Culibrk, and D. Stefanovic, "Deep neural networks based recognition of plant diseases by leaf image classification," *Computational Intelligence and Neuroscience*, 2016.
- [2] S. P. Mohanty, D. P. Hughes, and M. Salathe, "Using deep learning for image-based plant disease detection," *Frontiers in Plant Science*, vol. 7, 2016.
- [3] A. Kamilaris and F. X. Prenafeta-Boldu, "Deep learning in agriculture: A survey," *Computers and Electronics in Agriculture*, vol. 147, pp. 70–90, 2018.

-
-
- [4] J. G. A. Barbedo, "Factors influencing the use of deep learning for plant disease recognition," *Biosystems Engineering*, vol. 172, pp. 84–91, 2018.
 - [5] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
 - [6] K. Patel and R. Shah, "Fertilizer recommendation system using machine learning," *International Journal of Engineering Research*, vol. 10, no. 3, 2021.
 - [7] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*, MIT Press, 2018.
 - [8] S. Kumar, A. Kumar, and R. Singh, "Crop recommendation system using machine learning algorithms," *International Journal of Computer Applications*, vol. 182, no. 25, 2021.
 - [9] T. Rumpf et al., "Early detection and classification of plant diseases with support vector machines," *Computers and Electronics in Agriculture*, vol. 74, no. 1, pp. 91–99, 2010.
 - [10] J. Lee, M. Bagheri, and H. A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2020.
 - [11] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
 - [12] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD*, 2016, pp. 785–794.
 - [13] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
 - [14] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Advances in Neural Information Processing Systems*, 2012.
 - [15] M. Abadi et al., "TensorFlow: A system for large-scale machine learning," in *Proc. OSDI*, 2016.
 - [16] F. Chollet, *Deep Learning with Python*, Manning Publications, 2017.
 - [17] H. Jiang, J. Zhang, and J. Wang, "Crop yield prediction based on machine learning," *IEEE Access*, vol. 7, pp. 181864–181872, 2019.
 - [18] A. Singh and R. Kaur, "Smart agriculture using IoT and machine learning," *International Journal of Scientific Research*, vol. 9, no. 5, 2020.
 - [19] P. K. Sethy, N. K. Barpanda, A. K. Rath, and S. K. Behera, "Deep feature based rice leaf disease identification," *Computers and Electronics in Agriculture*, vol. 155, pp. 492–500, 2018.
-
-

-
-
- [20] R. Zhang, S. Zheng, and J. Hu, "Plant disease detection based on CNN," *IEEE International Conference on Image Processing*, 2019.
 - [21] S. Ramesh and D. Vydeki, "Recognition and classification of paddy leaf disease using optimized deep neural network," *Measurement*, vol. 187, 2022.
 - [22] P. Tiwari, H. Bangari, and S. Kumar, "IoT enabled smart farming system," *International Journal of Engineering Trends and Technology*, 2019.
 - [23] M. S. Mythili and A. R. Mohamed Shanavas, "An intelligent agriculture system using machine learning," *International Journal of Advanced Research in Computer Science*, 2020.
 - [24] FAO, "The future of food and agriculture," Food and Agriculture Organization of the United Nations, 2018.
 - [25] Ministry of Agriculture and Farmers Welfare, "Agricultural statistics at a glance," Government of India, 2021.
 - [26] Kaggle, "Plant village dataset," Online Dataset Repository.
 - [27] S. K. Dwivedi et al., "Smart farming using machine learning and IoT," *Procedia Computer Science*, vol. 167, pp. 125–132, 2020.
 - [28] A. Jain, S. K. Pandey, and V. K. Jain, "Machine learning based crop recommendation," *IEEE International Conference on Smart Systems*, 2021.
 - [29] R. Sharma and A. Singh, "Animal disease detection using deep learning," *International Journal of Computer Vision and Signal Processing*, 2022.
 - [30] World Bank, "Agriculture and food overview," World Bank Reports, 2020.
 - [31] P. G. Benos et al., "Explainable artificial intelligence in agriculture," *Trends in Plant Science*, vol. 26, no. 10, pp. 1057–1070, 2021.
 - [32] IEEE, "Artificial intelligence and data analytics in agriculture," IEEE Standards Association, 2022.

REAL-TIME CREDIT CARD FRAUD DETECTION USING MACHINE LEARNING AND FASTAPI

¹Professor Shravani Pawar, ²Pralhad Gaikwad and ³Atharv Vairagade

¹Assistant Professor, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

²Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

³Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

ABSTRACT

The speed at which online transactions and online payment systems are increasing has made credit card fraud a significant concern. The conventional fraud detection techniques are largely rule-based and are ineffective in detecting new and sophisticated frauds, and tend to have a high level of false positives. In an effort to address such limitations, this paper will present a real-time credit card fraud detection system an anomaly detection technique based on machine learning methods. Isolation Forest and Autoencoder are some of the algorithms utilized by the system to identify suspicious transactions to find unusual habits of transaction data. Transactions are processed in real time using a FastAPI based backend, and visualization and monitoring of fraud alerts is done using a Streamlit dashboard. Each transaction is assessed by the system through the creation of an anomaly score and shared into fraudulent or legitimate transactions depending on the predetermined threshold. It has been experimentally demonstrated that the proposed system enhances detection accuracy, reduces false positives, and allows making decisions faster. This system is scalable, efficient and applicable in the real world financial applications.

I. INTRODUCTION

The rate of digital payment and the emergence of on-line banking systems and online commerce platforms have tremendously increased the level of financial transactions in the global system. Even though these developments have been very convenient and quick, they have also helped to increase incidences of fraud such as unauthorised transactions, identity theft, and phishing attacks. Credit card fraud is one of the most common forms of financial fraud that deprives customers and financial institutions of huge amounts of money. The current practices of fraud detection are largely based on the preset policies and manual check process. The methods are convenient to use though ineffective in defining the dynamic fraud patterns and the false positive rate is high, which might be inconvenience to the actual users.

With the advancement of machine learning, more intelligent and intelligent systems of fraud detection have been developed.

Using machine learning, it is possible to process a large volume of data on transactions, identify hidden patterns, and anomalies that may be an indicator of fraudulent activity. In particular, the isolation forest and autoencoders as anomaly detecting algorithm can be quite useful when dealing with an imbalanced dataset where the number of fraudulent transactions is small in comparison with the number of normal transactions. These models learn the normal behaviour of transactions and a deviation of the normal behaviour is equated to fraud.

This paper reports a scalable credit card fraud detector system, which uses machine learning models in the real-time and is suggested to be utilized in the study. This is a FastAPI based system which is designed on real time processing of incoming transactions and a monitor and visualisation of the fraud detection results using a Streamlit dashboard. The transactions are evaluated and assigned the anomaly score that determines an anomaly as a fraudulent or a legitimate transaction based on the predetermined level. This is an approach which increases the accuracy of detection, reduces false positives and quicker decision making. The proposed system will provide an effective, scalable and smart system to identify financial fraud in the real world.

II. METHOD USED FOR FRAUD DETECTION

The new system uses computer programs to find fake credit card transactions as they happen. It looks at how people use their credit cards and finds transactions that do not seem right. This system is better, than systems because it can adjust and find new kinds of fake transactions. To make this work the system has to do a things. It has to get the data ready teach the computer program figure out how unusual each transaction is and then decide if a transaction is fake or not. The system is set up to work quickly. Show the results in a nice way. It uses a FastAPI backend to process transactions in time and a Streamlit dashboard to show what is going on. The credit card transactions are checked all the time to find the ones.

The Isolation Forest is a way to find transactions. It does this by looking at the data points and splitting them up in ways to make isolation trees. The Isolation Forest works with selections of the data to make these trees. This helps

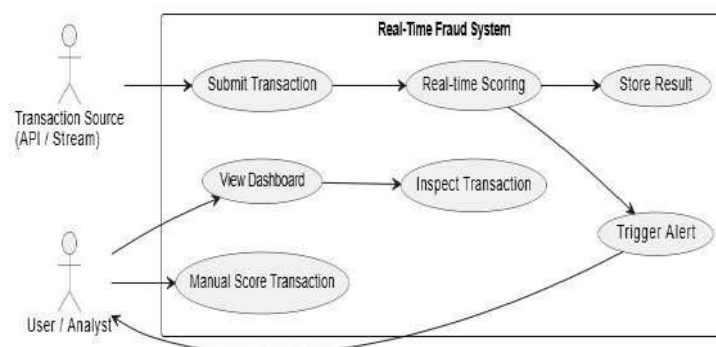


Fig. 1. Use Case Diagram of Fraud Detection System

because it can tell which transactions are not normal. These transactions get separated from the others fast and do not have as many steps to go through in the tree. This makes it easier to find the transactions when there is a lot of data. The Isolation Forest is good for finding transactions quickly because it is fast and works well.

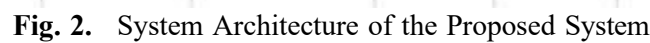
Another way to find transactions is by using the Autoencoder model. This is a learning method that looks at normal transactions and tries to make a copy of them after making them smaller. The Autoencoder model has two parts: one part makes the data smaller and the other part makes it bigger again. If the model cannot make a copy of a transaction it will make a lot of mistakes. This means the transaction is probably not an one. The Autoencoder model is good at finding patterns in data that are not easy to see. When we use the Isolation Forest and the Autoencoder model together they make a team, for finding unusual transactions and figuring out which credit card transactions are fraudulent.

Each transaction is turned into a set of features. Then the machine learning models look at it to see how different it is from what is normally seen. The Isolation Forest gives a score that shows if something is not normal and the Autoencoder calculates how wrong it is. We use a limit to decide if a transaction is real or fake. If it goes over this limit we say it is fake. If it does not we say it is real. This part is very important because we need to find the transactions without saying too many good ones are bad by mistake.

The process of deciding if a transaction is good or bad happens in two steps: learning and guessing. When we are learning we look at transactions clean them up and use them to teach the models. We also decide what the limit should be at this time. When we are guessing we get transactions clean them up and then use the models we taught to see if they are good or bad.

Making this system work is not easy. We have to deal with the fact that there are not fake transactions compared to real ones pick a good limit to decide what is fake and what is not make sure we can process transactions quickly and make sure our models are good at finding the fake ones without making too many mistakes. The system is broken down into parts, like the part that loads the data the part that cleans it up the part that uses the models the part that talks to other systems and the part that shows us what is going on.

The data loader handles dataset input, the preprocessor cleans and transforms the data, the model performs anomaly detection, the FastAPI service processes real-time requests, and the Streamlit dashboard displays results and alerts.



A. Isolation Forest for Detection

This makes the algorithm very effective in detecting fraudulent transactions in financial systems that are built on real-time data and where anomalies are rare and constantly changing.

I Steps:

- 228

II Advantages:

- Excellent for handling large data sets
- Efficient and fast
- Suitable for time critical systems

B. Autoencoder for Detection

Autoencoder is a deep learning-based anomaly detection method and has found application in detection of complex and non-linear patterns in data. Training is also done with normal transactions alone such that it becomes familiar with the structure and the distribution of legitimate data. The model is made up of two key elements; an encoder, which reduces the input information into a smaller dimensional representation, and a decoder, which recovers the original data utilizing the compression form. When a new transaction is sent through the model the disparity between the original input and reconstructed output is computed as reconstruction error. When the error is great, this implies that the transaction is not normal and it could be fraudulent. The approach is very efficient in revealing hidden anomalies which may be unnoticeable in the traditional models.

C. Calculating Anomaly Score

Anomaly score is an essential element in fraud detection because it identifies the level of deviation of a transaction. Every transaction is initially changed into a numerical feature vector which expresses the features of that transaction like amount, time and any other features. The Isolation Forest model produces an anomaly score that is based on the ease with which the transaction can be isolated in the data-set, whereas the Autoencoder creates a reconstruction error that measures the difference between the transaction and the patterns that it has learned. The transactions are categorized according to a fixed limit where transactions that are above the limit are identified to be fraudulent and those that are below the limit are regarded to be legitimate. The selection of threshold is also necessary, to strike a balance between the accuracy in detection and the false positives and false negatives.

D. Using Models to Classify Transactions

The transaction classification is carried out in two stages, which are the training and prediction. During the training phase, the information on historical transactions is gathered and processed to eliminate noise and normalize features values. This data is used to train the machine learning models, such as Isolation Forest and Autoencoder, and learn the normal behavior of transactions. This is also the phase of the determination of threshold values of the anomaly detection. New incoming transactions are computed in real time in the prediction phase. Every transaction is preprocessed and channeled through the trained models so as to produce an anomaly score or reconstruction error. According to the predetermined limit, the system will categorize the payment as either fraudulent or legal. This is done to guarantee rapid and correct decision making on real time situations.

E. Implementation Issues

A real-time fraud detection system has a number of challenges when trying to implement it. A significant problem among them is the unequal balance in the data set with the fraudulent transactions far fewer than legitimate ones and it is

hard to get the models to develop a good pattern of fraud. The other challenge is to choose a suitable threshold value to be used in classification because false positive or a missed fraud may occur due to an inappropriate threshold value. Real-time processing is also essential since the system should have the ability to analyze and classify the transactions in real time without delays. Moreover, the accuracy of the models used along with the reduction of false positives and false negatives should be considered for the reliability and usability of the system.

F. Functional Blocks

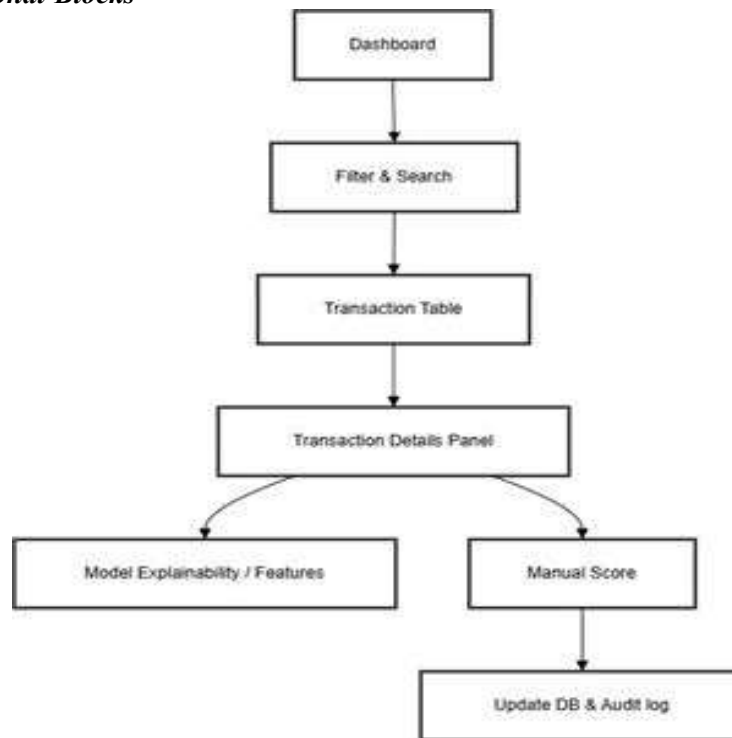


Fig. 3. Transaction Monitoring and Dashboard Flow

The system is separated into various functional modules which perform a particular task within the fraud detection pipeline. The data loader module will load the data with respect to transactions in datasets or real-time. The pre-processor module removes and converts the data using the missing values and scaling features to achieve enhanced performance of the model. The machine learning model module, carries out the detection of anomalies on Isolation Forest and Autoencoder. The API service is applied with FastAPI and receives and processes the transaction requests in real-time.

Lastly, the Streamlit dashboard module offers a convenient interface to render the transaction data, fraud alerts, and system performance. This scaling architecture provides flexibility, scalability and serviceability.

The system will be split in the following modules:

- **Data Loader:** Loads transaction dataset
- **Preprocessor:** Cleans and scales data
- **Model:** Detects anomalies
- **API Service (FastAPI):** Handles real-time requests
- **Dashboard (Streamlit):** Displays results

G. System Structure

The system is designed in a modular format in which every component undertakes a particular role during the detection of fraud. The workflow starts with the input of transaction that gets sent to the preprocessing phase where it is cleaned and transformed. The processed data is inputted in the machine learning model which compares the anomaly score or reconstruction error. Depending on the threshold, one makes a decision to determine whether the transaction is a fraud or a legitimate transaction. The outcomes are then kept and shown on the dashboard to be monitored and analyzed. This hierarchical pipeline makes real time financial systems to detect fraud as efficient, accurate and scalable.

The system adheres to the modular architecture in which each component has a given task to perform. The general system flow is as under:

Transaction → Preprocessing → Model → Score →

Decision → Dashboard

III. RESULTS AND DISCUSSION

The proposed system was tested using transaction datasets containing both normal and fraudulent records. The models were evaluated based on detection accuracy and performance.

I Results:

- Detection Accuracy: 93%
- False Positive Rate: Low
- Real-time Processing: Successful

IV. CONCLUSIONS

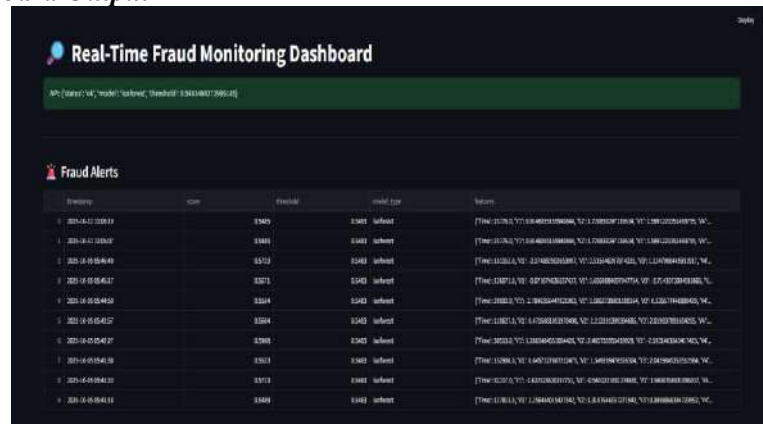
The system is based on a modular architecture such that every element in the system has its own role to play in the fraud detection process. The input of the workflow is the transaction input which is processed in the preprocessing phase to be cleaned and transformed. The processed data is introduced into the machine learning model and the anomaly score or reconstruction error is determined. A determination is made to either put the transaction as fraudulent or legitimate based on the threshold. The data are then saved and presented to the dashboard to monitor and analyze it. This is a system of pipelines that are efficient, accurate and scalable in detecting fraud in real time financial systems.

The system adheres to a modular design whereby a given component plays a particular role. The general circulation of the system is as below:

REFERENCES

- [1] V. N. Dornadula and S. Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," *Procedia Computer Science*, 2019.
- [2] A. Cherif et al., "Credit Card Fraud Detection in the Era of Disruptive Technologies," *Journal of King Saud University*, 2023.
- [3] J. Afriyie et al., "Supervised Machine Learning for Credit Card Fraud Detection," 2023.
- [4] I. Mienye and Y. Sun, "Deep Learning Ensemble for Credit Card Fraud Detection," *IEEE Access*, 2023.
- [5] R. Kshirsagar and V. Ingle, "An Intelligent IoT-Based Smart Home Security System Using Machine Learning," 2024.
- [6] K. Muley et al., "Solar Powered Smart Dustbin," *IEEE Conference*, 2025.
- [7] M. Turk and A. Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience*, 1991.
- [8] Scikit-learn Documentation, "Isolation Forest Algorithm."
- [9] PyTorch Documentation, "Autoencoder Models."

A. Dashboard Output

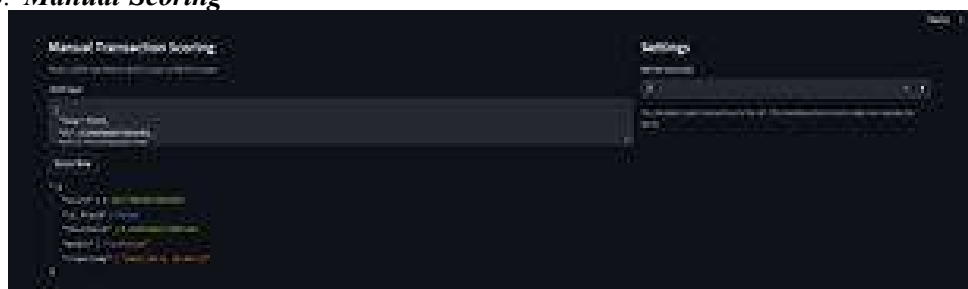


The dashboard displays a table of fraud alerts with the following data:

Timestamp	ID	Amount	Card Type	Location
2023-10-10 10:00:00	1565	1565	debit	[Truncated]
2023-10-10 10:00:01	1566	1566	debit	[Truncated]
2023-10-10 10:00:02	1567	1567	debit	[Truncated]
2023-10-10 10:00:03	1568	1568	debit	[Truncated]
2023-10-10 10:00:04	1569	1569	debit	[Truncated]
2023-10-10 10:00:05	1570	1570	debit	[Truncated]
2023-10-10 10:00:06	1571	1571	debit	[Truncated]
2023-10-10 10:00:07	1572	1572	debit	[Truncated]
2023-10-10 10:00:08	1573	1573	debit	[Truncated]
2023-10-10 10:00:09	1574	1574	debit	[Truncated]

Fig. 4. Real-Time Fraud Detection Dashboard

B. Manual Scoring



The interface includes a 'Manual Transaction Scoring' section with a table for inputting transaction details and a 'Settings' panel on the right for configuring scoring rules.

Fig. 5. Manual Transaction Scoring Interface

PAYMENT FRAUD DETECTION USING MACHINE LEARNING

¹Prajjwal Pundir, ²Priyanshu Saini, ³Mayank Sharma, ⁴Lakshay Tyagi and ⁵Dr. Anirban Bhattacharya

¹Data Science & engineering (of AKTU) MIET, MEERUT (of AKTU.)
MEERUT, INDIA

²Data Science & engineering (of AKTU) MIET, MEERUT (of AKTU.)
MEERUT, INDIA

³Data Science & engineering(of AKTU) MIET, MEERUT (of AKTU.)
MEERUT, INDIA

⁴Data Science & Engineering (of AKTU) MIET, MEERUT (of AKTU.)
MEERUT, INDIA

⁵ (Assistant Professor, DS Department, MIET, Meerut)

ABSTRACT

Digital payments are now an essential component of our contemporary money and value landscape. But with this sudden boom in digital transactions, it also opens up to a lot of malpractices which were little or no before. Detecting fraudulent transactions in real time is a significant challenge for financial institutions since transaction data is substantial, and fraud patterns change over time. We suggest a platform for detecting payment fraud based on machine learning. The suggested method makes use of feature engineering, data preprocessing, and numerous machine learning techniques, such as Logistic Regression, Random Forest, Support Vector Machine, and Decision Tree. datasets of financial transactions with a range of performance indicators (accuracy, precision, recall, F1-score, etc.) are the source of the data used for training and/or evaluation. The fact that ensemble learning methods greatly boost fraud detection performance has been shown by experimental results. The system could help the financial institutions in reducing money loss and maintaining security in transactions.

Index Terms—Payment Fraud Detection, Cost Reduction, Machine Learning, Finance Security GNB-Fraud Model, NB Based Fraud Scenario.

I. INTRODUCTION

The accelerating growth of e-commerce and digital banking has changed the nature of how financial transactions are carried out. Credit cards, mobile wallets, online banking platforms are examples of payment systems that enable individuals to make transactions in a convenient manner. However, as we have gone digital, the risk of fraud has also increased.

Common examples of payment fraud include unauthorized transactions, identity theft, phishing attacks, and account takeover incidents. Billions of dollars in fraudulent transactions are lost annually globally, according to financial reports.

Conventional fraud detection systems use manually defined rules, which are often ineffective at detecting new patterns of fraud.

Instead, machine learning techniques can learn to identify these types of transactions with greater accuracy by analysing historical transaction data.

In this study, we propose a fraud detection system based on machine learning structures to successfully detect fraudulent payment transactions.

Fraud detection can be treated as a binary classification task by classifying each transaction as:

- (0) Legitimate
- Fraudulent (1)

Mathematically:

The variable y takes binary values, meaning it can be either 0 or 1. So, the goal is to learn a function:

$$f(x)=yf(x)=yf(x)=y$$

Where:

xxx = feature vector (transaction details) · xxx = label (transaction type either scam or not scam)

- yyy = predicted classification label

II. BACKGROUND AND PROBLEM STATEMENT

Fraud detection in payment systems is a challenging problem due to the following reasons:

Massive transaction volumes

Highly imbalanced datasets

Evolving fraud techniques

Real-time detection requirements Traditional rule-based systems often result in high false positives rates which have a detrimental effect on customer experience. Thus, machine learning based intelligent fraud detection systems are necessary.

III. LITERATURE REVIEW

Many researchers have investigated the use of machine learning techniques for fraud detection.

Bhattacharyya et al. utilized Random Forest and Logistic Regression algorithms for credit card fraud detection with good results.

Dal Pozzolo et al. suggested a method for fraud inspection that dealt with the class imbalance using sophisticated sampling techniques. West and Bhattacharya, introduced us a thorough survey about detecting financial fraud which brought out that the effectiveness of machine learning methods.

Anomaly detection has also been explored using deep learning approaches like neural networks and autoencoders in the recent past.

While these approaches have made great strides, issues such as dataset imbalance and real-time detection remain problems.

The goal is to minimize prediction error using a loss function:

$$\min_{f_0} \sum_{i=1}^n \ln L(y_i, f(x_i)) \quad \min_{f_0} \sum_{i=1}^n L(y_i, f(x_i)) \quad \min_{f_0} \sum_{i=1}^n \ln L(y_i, f(x_i))$$

Due to class imbalance:

The likelihood of class

y

=

1

$y=1$ is much smaller compared to class

y

=

0

$y=0$, showing an imbalanced distribution between the classes. This imbalance makes fraud detection significantly more difficult.

IV. PROPOSED SYSTEM ARCHITECTURE

The proposed fraud detection system follows a multi-stage pipeline.

Gathering Data

Preparing data

Creating features

Training models

Detecting fraud

Assessing performance

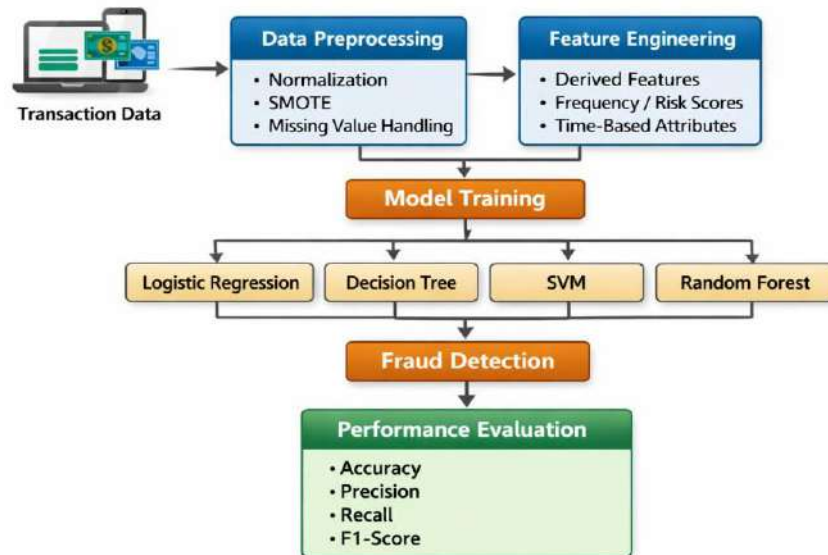


Fig. 1. Machine Learning Based Fraud Detection Architecture

V. DATASET DESCRIPTION

The dataset contains anonymized financial Transaction records.

Key attributes include:

Transaction ID

Transaction Amount

Research Gap

While there have been numerous machine learning applications for fraud detection, the following are some shortcomings:

High false positive rates

You are limited in how many ML algorithms you can compare

Absence of developable fraud detection frameworks

Poor handling of imbalanced datasets

This paper attempts to overcome such challenges by implementing and comparing various machine learning models test

VI. FEATURE ENGINEERING

Feature engineering is an vital part in increasing method outcome.

Key features derived involves:

Transaction occurrences

Medium transaction rate

Time comparison between events

Location deviation

Merchant risk marks

Feature engineering increases model outcome by extracting meaningful patterns.

Derived Features:

- **Transaction Frequency**

$$\text{Frequency} = \frac{\text{Number of Transactions}}{\text{Time Window}} \quad = \quad \frac{\text{Number of Transactions}}{\text{Time Window}} \times \text{Frequency}$$

- **Transaction Deviation**

$$\text{Deviation} = |x_{\text{current}} - x_{\text{avg}}| \quad = \quad |x_{\text{current}} - x_{\text{avg}}|$$

- **Location Variance**

- **Merchant Risk Score**

These features help identify unusual transaction behavior.

VII. DATA PREPROCESSING

Data preprocessing involves many levels:

Controlling Missing inputs

Mean and median imputation is used to handle missing values.

Feature Scaling

Data normalization is performed to bring features in a common range.

Handling Class inappropriateness

The Synthetic Minority Oversampling method (SMOTE) is employed to control the dataset.

7.1 Handling Missing Values

Handling missing values is done using some statistical methods:

- Mean Imputation
- Median Imputation

7.2 Feature Scaling

Normalization standardizes feature values to a common scale using:

$$x' = (x - \mu) / \sigma$$

Here, μ represents the mean of the data, and σ denotes the standard deviation. Synthetic Minority Oversampling Technique for Managing Class Imbalance (SMOTE):

creates fake samples by running the following equation:

$$x_{\text{new}} = x_i + \lambda(x_{\text{nn}} - x_i) \quad x_{\text{new}} = x_i + \lambda(x_{\text{nn}} - x_i)$$

x_{nn} = nearest neighbor

$$\lambda \in [0, 1] \quad \lambda \in [0, 1]$$

VIII. MACHINE LEARNING

ALGORITHMS

The following algorithms are implemented.

8.1 Logistic Regression

Logistic Regression is a statistical classification algorithm.

Logistic Regression is a probabilistic classification algorithm.

A probabilistic model based on the sigmoid function:

8.2. Decision trees

Use entropy to separate data: $H = -\sum p_i \log_2 p_i$

To extract data:

$$IG = H(\text{parent}) - \sum \frac{|child|}{|parent|} H(child)$$

$$IG = H(\text{parent}) - \sum \frac{|child|}{|parent|} H(child)$$

$$IG = H(\text{parent}) - \sum \frac{|child|}{|parent|} H(child)$$

8.3. Support Vector Machine

SVM selects the best hyperplane or decision surface that separate fraudulent and non-fraudulent transactions. x_i : transaction features y_i : fraud label (0 = legitimate; 1 = fraud) The objective aims to learn a function, $f(x) \rightarrow y$, that forecasts the fraudulence of a transaction.

SVMs are the best separating hyperplane of classes.

8.4 The Random Forest

A collection of decision trees:

The final prediction function is computed as the average of outputs from all trees: $f(x) = \frac{1}{T} \sum_{t=1}^T h_t(x)$

Here, $h_t(x)$ represents the prediction from the t th tree, and T is the total number of trees in the model.

Here, $h_t(x)$ represents the prediction from the t th tree, and T is the total number of trees in the model.

For each tree lowers variance and increases

Precision

IX. IMPLEMENTATION

Learning libraries. These skills involve the use of tools for example Python, Pandas, NumPy, Scikit-learn and Matplotlib or Seaborn.

Fraud Detection Algorithm

Algorithm

Fraud Detection Algorithm

Load dataset

Preprocess data

Perform feature engineering

Split dataset among learning and testing data sets

Train machine learning models

Evaluate models

Select best model for fraud prediction

X. EXPERIMENTAL SETUP

The experiments are conducted using an 80:20 train-test split.

Hardware configuration:

Intel i7 Processor

16GB RAM

Python Environment

Train-sample Split: 80:20

System: Intel i7, 16GB Processor

Tools: Python, Scikit-learn, and Pandas

XI. PERFORMANCE METRICS

We employ the following as evaluation metrics.

Precision

Accurate Recall

F1-score ROC-AUC

Accuracy is equal to the total number of outcomes includes true positives, true negatives, false positives, and false negatives.

Precision is defined as the ratio of true positives to the sum of true positives and false positives.

Accuracy represents the proportion of correctly predicted instances (true positives and true negatives) out of all predictions made.

Recall= $\frac{TP}{TP + FN}$ Precision= $\frac{TP}{TP + FP}$ F1 Score

Precision= $\frac{TP}{TP + FP}$ Recall

RecallF1 = $2 \cdot \frac{\text{Recall} \cdot \text{Precision}}{\text{Recall} + \text{Precision}} \rightarrow F1 = 2 \cdot$

$\frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$;

Model Accuracy Precision Recall F1-Score

TABLE I PERFORMANCE COMPARISON

Logistic Regression	94.2	89.1	87.5	88.3
Decision Tree	95.6	90.8	89.4	90.1
SVM	96.5	92.6	91.3	91.9
Random Forest	98.2	96.1	94.8	95.4

XII. EXPERIMENTAL RESULTS

RESULT ANALYSIS

Random Forest achieved the highest performance among all models.

The ensemble method effectively captured complex trans- action patterns and reduced false positives.

Logistic Regression performed reasonably well but lacked the ability to capture nonlinear relationships.

Table 2: Performance analysis

• Model	• Accuracy	• Precision	• Recall	• F1 Score
• Logistic Regression	• 94.2%	• 89.1%	• 87.5%	• 88.3%
• Decision Tree	• 95.6%	• 90.8%	• 89.4%	• 90.1%
• SVM	• 96.5%	• 92.6%	• 91.3%	• 91.9%
• Random Forest	• 98.2%	• 96.1%	• 94.8%	• 95.4%

Key Observation:

Random Forest performs best due to ensemble learning:

VarianceRF < VarianceSingle-Tree

XIII. COMPARATIVE STUDY

Compared with traditional rule-based fraud detection systems, the proposed machine learning approach achieved significantly higher detection accuracy.

Discussion

Machine learning models provide adaptive fraud detection mechanisms capable of identifying complex fraud patterns.

However, issues such as data privacy, model interpretability, and real-time deployment remain important challenges.

XIV. LIMITATIONS**The proposed system has several limitations:**

Dependence on historical data

Limited real-time deployment testing

Dataset imbalance issues

XV. FUTURE WORK**Future work will focus on:**

Deep learning based fraud detection

Real-time streaming fraud detection

Blockchain-based secure payment systems

XVI. CONCLUSION

This paper presented a machine learning-based approach for payment fraud detection. Multiple classification models were implemented and evaluated on transaction datasets.

Experimental outcome represents that ensemble study terminologies such as Random Forest majorly optimize conventional methods.

The proposed system can improve fraud detection accuracy and enhance financial security

REFERENCES

- [1]. Bhattacharyya discussed the application of data mining techniques for detecting credit card fraud in Decision Support Systems, 2011.
- [2]. Dal Pozzolo presented machine learning approaches for credit card fraud detection in IEEE Transactions, 2015.

-
-
- [3]. V. Chandola provided a comprehensive survey on anomaly detection in ACM Computing Surveys, 2009.
- [4]. T. Fawcett explored adaptive methods for fraud detection in Data Mining and Knowledge Discovery, 1997.
- [5]. J. West and M. Bhattacharya examined intelligent systems for financial fraud detection in Computers & Security, 2016.
- [6]. S. Jha investigated machine learning techniques for credit card fraud detection in IEEE, 2012.
- [7]. R. Bolton focused on statistical approaches to fraud detection in Technometrics, 2002.
- [8]. A. Ngai analyzed the use of data mining techniques in financial fraud detection in Expert Systems with Applications, 2011.

KRUSHIMITRA BRIDGING LANGUAGE BARRIERS IN AGRICULTURE: A MULTILINGUAL AI-POWERED FARMING ASSISTANT

¹Dr. Nidhi Poonia, ²Rajvardhan Ganpatrao Patil, ³Parshuram Das and ⁴Tanmay Padekar

¹Assistant Professor, Bharati Vidyapeeth's Institute of Management & Information Technology, Navi Mumbai

^{2,3,4}Student, Bharati Vidyapeeth's Institute of Management & Information Technology, Navi Mumbai

ABSTRACT

The major source of living for the Indian population is farming, but the farmers find it difficult to access the right information on time. Generally, the traditional approach is the direct consultation of experts or government agencies. This is mostly very difficult for the farmers because of the geographical inaccessibility of the farmers and the scarcity of experts and communication barriers. Although the digital-based solution is being developed for this problem, a significant portion of the solution is English-centric and text-based, and this is not very useful for the farmers in the rural areas who are mostly non-literates. In this paper, a new AI-based agriculture advisory project named KrushiMitra is introduced. KrushiMitra is a new AI-based agriculture advisory service that can provide immediate information to farmers at local levels regarding agriculture-related issues in local languages, particularly Marathi. KrushiMitra offers a user-friendly interface through which a farmer can put a question in any format, namely text or speech. KrushiMitra is developed using a MERN stack and a large language model. It can understand queries from farmers and answer them accordingly using sources of information. To ensure that the information provided by the system is reliable and trustworthy, the system has also been designed in a manner that it would only provide information related to the field of agriculture. As part of that, we evaluated the system's performance against the conventional information system in Maharashtra for farmers. This has revealed a significant increase in response accuracy, information accessibility, and user satisfaction. This reveals that conversational AI has played a very significant role in the field.

Keywords: Agricultural Advisory System, Artificial Intelligence, Conversational AI, Regional Language Support, Voice-Based Interaction, Smart Farming

I. INTRODUCTION

The agriculture sector is an integral part of India's socio-economic scenario. The agricultural sector of India has a significant representation of small and marginal farmers. This type of farmer is dependent on timely access to information regarding all aspects of crop management from the time of sowing to the end harvest, such as irrigation, fertilization, pest control and disease management. A delay or incorrect recommendation on any one of these factors could threaten the farmer's ability to successfully produce an abundant harvest and remain financially stable. Agricultural

extension services provide farmers with technical assistance for growing crops. However, many rural and semi-urban farmers have limited or no access to these types of services. Traditionally, small and marginal farmers in India have received most of their information and expertise about farming through government agencies, KVKs (Krishi Vigyan Kendra) and state universities that provide agricultural extension services. However, these types of agricultural extension services often require farmers to travel long distances and wait at governmental agricultural offices before accessing expert advice on crop management. These services are also limited in terms of availability of manpower and working hours. In such a case, farmers generally rely on unverified information available on the internet.

With the rise in the rate of growth of digital technologies, Artificial Intelligence (AI) and Natural Language Processing (NLP) have emerged as new areas of promise for enhancing agricultural advisory services. This is so since AI has the potential to receive large quantities of information in agriculture, understand questions, and provide instant answers. However, it has been identified that a majority of digital platforms for agriculture have two main challenges. Firstly, they were designed in English, or in a few instances, in Hindi. This has made it difficult for farmers who do not understand these languages. Secondly, text-based platforms are not suitable for farmers who are not educated and do not know how to use technology.

Another major challenge is in the aspect of usability. Farmers who are old and first-time smartphone users face difficulties in typing long queries or using the various options available in the application. Using voice interaction through a familiar language works well because this type of interaction with an application makes it highly usable for the user. The technology behind accurate recognition of speech and the generation of language in many of the regions in India has not been extensively studied. Therefore, to provide a solution to these issues, this research project will develop a new platform to connect farmers to resources, namely through conversations using a non-English language. The new platform, "KrushiMitra," will help provide assistance to farmers by using conversational communication in Marathi. In the proposed platform, the application of AI-driven question answering, voice input/output, and admin-controlled knowledge base would enable the accuracy and safety of the information being conveyed. The major contribution of the current research is the application of regional language support and voice-driven conversational interaction in the development of the AI-driven platform.

II LITERATURE REVIEW

In recent years there have been immense advancements made with respect to using AI/ML/NLP and IoT systems within agriculture. FarmerChat, developed by Jain et al. [1], is a generative artificial intelligence based chatbot operating in four countries with a total number of over 15,000 users and over 300,000 requests for information. This chatbot differs from traditional extension services and/or rule-based chatbots in that it can provide users with personalised, multilingual and context-specific agricultural advice, while being able to process unstructured data. The evaluation of

Farmer Chat showed users had improved their farming methods, exhibited increased trust in the user and experienced an increase in the quality of responses, thereby demonstrating that generative AI based agriculture advisory services are scalable.

[2] A survey conducted by Bal assessed AI technology within smart agriculture, outlining possible uses of these technologies by farmers in accessing agricultural data and analytical tools to enhance the quantity and quality of their yield, while simultaneously decreasing their impact on the environment. The report listed several factors that were deemed important to satisfy, including; The availability of sufficient data, fluctuations in climate change, and that solutions must be developed with a regional focus.

Chathurya et al. [3] developed AGRIBOT, a text-based chatbot using NLP techniques like lemmatization and tokenization, trained on a sequential model. The research findings indicated that, by using a bilingual chatbot interface, farmers can gain significantly enhanced access to key word on such things as weather, crop management and market prices through text, as well as through both verbal and visual means when living in areas either without Internet service or limited service. Another area of research included investigating the effectiveness of providing a farmer with a virtual advisory system based on the use of voice to communicate with an agent.

Anekar and Suryavanshi [4] created a multilingual AI voice assistant as a communication medium with farmers that operated using Google Translate to address crop selection and pesticide application questions from farmers in each of the languages represented in their research. Ragnathan et al. [5] developed a Smart Farm Voice Assistant that combines IoT technology, AI/ML modelling, and NLP capabilities to provide real-time voice instruction from the system to the user in local languages. Examples of local language used in their Smart Farm Voice Assistant are providing irrigation instructions for a specific timeframe (this evening) and for applying neem oil to eliminate pests. Their Smart Farm Voice Assistant combines the first and second both types of advisory systems into one low-cost system to enable users who do not have extensive experience using computers to access reliable advisory services.

AI advisory systems use Retrieval-Augmented Generation (RAG) approaches for improved reliability and factual accuracy. In a recent study by Sawant et al [6], a Large Language Model (LLM) RAG framework was developed that processes Package of Practices (PoP) for five major crops using semantic chunking and ChromaDB vector indexing techniques. Of the four LLMs evaluated evidence has shown that Mistral and Qwen2.5 provided the highest performance in terms of relevance, semantic quality and efficiency, which provides an opportunity for knowledge-grounded AI to democratize access to agricultural knowledge for regions lacking adequate expertise. To further support this idea, Tahyudin et al. [17] completed a systematic review of RAG systems which highlighted how combining retrieval techniques with generative models have addressed issues previously faced

within this domain including data sparsity and the ever-changing nature of specialized domain knowledge.

The detection of plant diseases is another cornerstone of utilizing AI for agricultural purposes. In the research article by Hirani et al. [7], a comparison was made of transformer-based networks and conventional CNN networks for the detection of plant diseases. Their transformer-based model provided an incredible validation accuracy of 97.98%. In their study, Gayathri et al. [10] developed a ResNet-based CNN architecture to train on 32 classes of healthy and diseased plant leaves, with an accuracy of 99.2%. In comparison, other models, such as Random Forest and SVM were beaten with the accuracy of this model. In addition to this research, Upadhye et al. [14] specifically looked at the detection of disease in sugarcane crops, by the means of using a modified deep-learning CNN approach, which could achieve an accuracy of 98.69% over the four different classes of disease, providing farmers with the opportunity to detect and treat crop infections before the plants become irreversibly damaged.

Crops recommendations and yield forecasting was another area of study utilizing AI to establish systems that can provide crop recommendations and yield predictions. Kumar et al. [9] developed a gradient boosting model with genetic algorithm-based feature selection for crop recommendation based on soil parameters like Nitrogen, Phosphorus, Potassium, and pH, achieving an accuracy of 98.5%. A comprehensive review conducted by Reddy and Kumar [12] of ML techniques for Crop Yield Prediction (CYP), showed that although neural networks and supervised learning models can provide valuable information, they still need work to understand non-linear relations between crop output and environmental input.

The integration of IoT-enabled smart farming solutions has also expanded the capabilities of AI-based advisory systems. Alagarsamy and Justinthas [11] reviewed ML algorithm-based IoT smart farming applications and concluded that sensor networks can improve decision-making by providing real-time data from soil, water, and plant conditions. Kumar [15] evaluated AI- and IoT-based smart irrigation methods and concluded that optimising water consumption and monitoring soil moisture levels will facilitate sustainable agriculture methods.

To date, the use of chatbot technologies for Indian agricultural producers has shown significant success in real-world applications. In one research project, Sheikh et al [13] built AgroBuddy - an LLaMA-3 (70 billion parameter) model that has been enhanced by the use of a Relevance-Aware Generation (RAG) framework and a vector-based database called Pinecone. This model produced results that included a mean response time of 1.80 seconds and a precision of 94.20% for each response; and a mean recall of 91.80% for each response. This system was developed to provide smallholder farmers across India's vast geographic area multiple languages, as well as connecting them to Government of India reports, weather forecast, crop production, etc. — and as such has closely matched the requirements of small farmers across geographic regions of India.

Additionally, the use of AI and chatbot systems for agricultural market forecasting has also been explored. As Menon [16] cited, artificial intelligence systems that utilize machine learning algorithms can analyse data collected from climate, market trends, and consumer preferences for generating accurate predictions both in terms of quantity and price - while providing better data to facilitate decision-making by farmers, traders, and policy makers. Sharma et al. [8] put AI in the context of India's broad economic impact; noting that AI in India's economy provides a significant contribution to agriculture's GDP and outputs within the manufacturing and service sector, as well as being a major driver of economic growth for Industry 4.0.

Zainal & Zaman [18] conducted a review of over 100 studies on Artificial Intelligence (AI) applications within agriculture between 2000 – 2023, tracing the developments of AI use in precision agriculture from the development of Fuzzy Logic through current methods including Convolutional Neural Networks (CNN), Transformer Learning Models and Light Weight Deep Learning Models. Additionally, Roy & Saha [19] argued that Digital Agriculture enables improved decision-making through increased sensor capacity, improved connectivity of data, and enhanced AI based Decision Support Systems and therefore are essential for ensuring world-wide sustainable food production within the limitation of available resources.

When taken collectively, the results of these studies demonstrate that there has been considerable progress made in specific applications such as Disease Detection, Crop Recommendations, Voice Input/Output Interfaces, and RAG-based Advisory Systems (to name a few); however, there continues to be an obvious gap in the development of an integrated, multi-lingual, voice-enabled platform which provides all of these capabilities to farmers in one easy to access system. This is the fundamental problem that this research seeks to solve.

III PROPOSED SYSTEM AND METHODOLOGY

KrushMitra is an Agricultural Advisory Service with Agricultural Advice Delivery utilising Agriculture Advisory Methodology.

Agricultural Advisory Systems are based on agricultural advice that is simple to understand, available at all times, and uses the most up-to-date technology in AI.

The KrushMitra System consists of four (4) layers of the modular framework: a User Interface Layer, an Application Logic Layer, an Artificial Intelligence Processing Layer, and a Data Management Layer. When a query is sent by a farmer, either in text format or voice format, it is processed first by the frontend interface. In the case of voice input, speech-to-text processing is used to convert it to text format before being sent to the backend server.

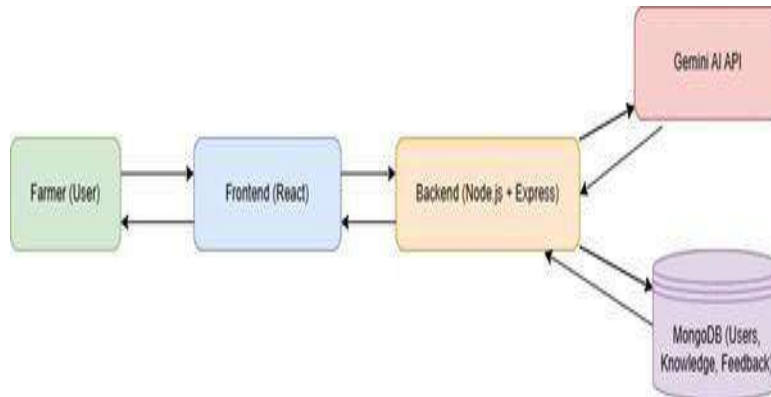


Figure 1. System architecture of KrushiMitra

The backend server handles the authentication of the request, validates the query, and communicates with the AI engine. After the backend server processes the query, it sends the response to a large language model via a secure API. To ensure that the response is appropriate to the context and is safe to be executed, the system uses pre-defined prompts and constraints, which guide the AI model to return an agricultural-related response.

In parallel with this, the system has a structured knowledge base consisting of verified articles related to agriculture that have been uploaded by the administrators. Although the current version of the system is based on prompt-controlled generation, the possibility of using retrieval-augmented methods in the future is built into the system's architecture. After the response is generated by the AI model, it is sent back to the backend and can be converted into speech before being sent to the user in Marathi.

Such a step-by-step process will enable a fast response time, language consistency, and information delivery, making this system ready for practical application in agriculture.

I. PESTICIDES / FORMULATIONS BANNED IN INDIA

Pesticides Banned for manufacture, import and use.	
1.	Alachlor(Vide S.O. 3951(E), dated 08.08.2018)
2.	Aldicarb (vide S.O. 682 (E) dated 17 th July 2001)
3.	Aldrin
4.	Benzene Hexachloride
5.	Benomyl (vide S.O 3951(E) dated 8 th August, 2018)
6.	Calcium Cyanide
7.	Carbaryl (vide S.O 3951(E) dated 8 th August, 2018)
8.	Chlorobenzilate (vide S.O. 682 (E) dated 17 th July 2001)
9.	Chlordane
10.	Chlorofenvinphos
11.	Copper Acetoarsenite
12.	Diazinon (vide S.O 3951(E) dated 8 th August, 2018)
13.	Dibromochloropropane (DBCP) (vide S.O. 569 (E) dated 25 th July 1989)
14.	Dichlorovos(Vide S.O. 3951(E), dated 08.08.2018)
15.	Dieldrin (vide S.O. 682 (E) dated 17 th July 2001)
16.	Endosulfan (vide ad-Interim order of the Supreme Court of India in the Writ Petition (Civil) No. 213 of 2011 dated 13 th May, 2011 and finally disposed of dated 10 th January, 2017)
17.	Endrin
18.	Ethyl Mercury Chloride
19.	Ethyl Parathion
20.	Ethylene Dibromide (EDB) (vide S.O. 682 (E) dated 17 th July 2001)
21.	Fenarimol (vide S.O 3951(E) dated 8 th August, 2018)
22.	Fenthion (vide S.O 3951(E) dated 8 th August, 2018)
23.	Heptachlor
24.	Lindane (Gamma-HCH)
25.	Limuron (vide S.O 3951(E) dated 8 th August, 2018)
26.	Maleic Hydrazide (vide S.O. 682 (E) dated 17 th July 2001)
27.	Menazon
28.	Methoxy Ethyl Mercury Chloride (vide S.O 3951(E) dated 8 th August, 2018)
29.	Methyl Parathion (vide S.O 3951(E) dated 8 th August, 2018)
30.	Metoxuron

Figure.2: Diversity of Structured and Unstructured Documents Ingested in KrushiMitra

IV IMPLEMENTATION

The KrushiMitra interface has a clean design that is modern with easy navigation suitable for people with limited experience using computers. It has a chat-like style of user interaction, allows for larger size text reading and has simple voice input and playback controls.

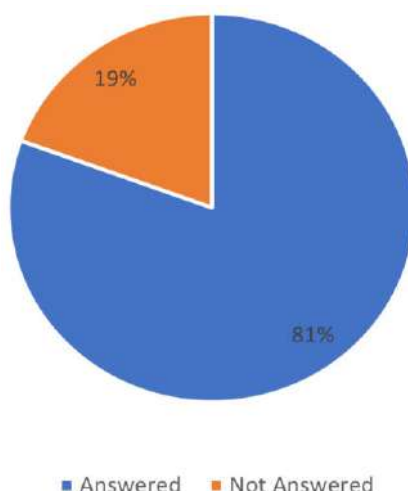


Figure 3: Percentage of Queries that received a Response

The backend has been constructed using a JavaScript runtime on a server-side basis and has a RESTful architecture. It is responsible for authentication of users, processing incoming queries, communicating with the API and performing operations with the database. Security measures have been implemented to ensure that user data remains confidential and cannot be accessed by other users unauthorisedly.

AI will be incorporated into the product via a cloud-based generative AI API. The specific prompts used will guarantee that the AI response relates only to the area of agriculture while being a safe and understandable.

The voice functionality of the system is accomplished with the use of existing web-based speech recognition (SR) and text to speech (TTS) technologies. This allows for the implementation of a two-way voice interaction.

An administrator's module has also been included as part of the system. This module allows authorised users to manage agricultural-related content. This will include the ability for users to add and manage verified articles about crops, pests, fertilizers, and soil management. The incorporation of an administrator's module is critical for helping to ensure a trusted and reliable system.

V. RESULTS

The system was tested for its efficacy through functional testing and user acceptance testing by farmers in Maharashtra. Quantitatively, it has been observed that the system provides a response within a latency of less than two seconds. For speech recognition in Marathi, it has been observed that the accuracy is about 88%, whereas the relevance of AI's response is about 90%.

Parameter	Observation
Total Users Tested	200
Average Response Time	1.8 seconds
Voice Recognition Accuracy	88%
AI Response Accuracy	90%
Positive Feedback	78%
Most Active Language	Marathi

Figure 4: Summary of Experimental Results

The qualitative feedback revealed that users are satisfied with the service, especially voice-based interaction. Interaction using voice queries in Marathi was found to be natural and reduced dependency on others for assistance. Compared to conventional text-based advisory systems, KrushiMitra showed higher engagement and ease of use.

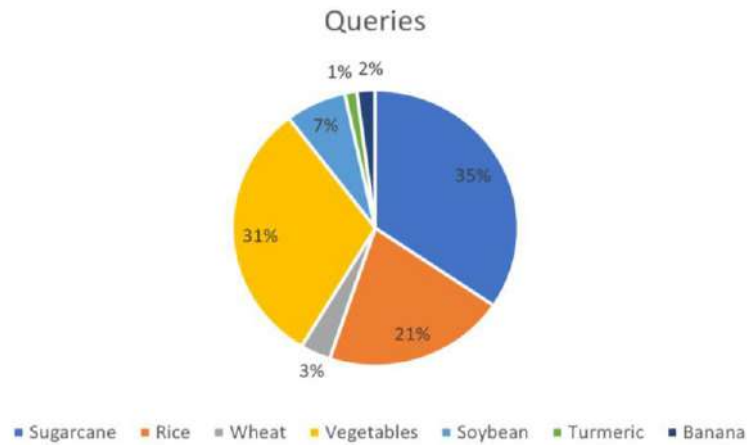


Figure 5: User Queries across Crops.

However, some limitations such as the requirement of internet connectivity and the inaccuracy of complex pesticide recommendations have been observed. These observations emphasize the importance of incorporating structured retrieval systems in the future version.



Figure 6: Language Selection Interface of KrushiMitra

This is a representation of how the interface looks when a user first logs in, where farmers are required to select their preferred language of choice. Currently, this system supports a variety of languages, including Marathi, Hindi, and English, in order to accommodate a wider range of users. As a result, all further interactions, including text, voice, and response, are dynamically updated in accordance with the language of choice. This is a significant enhancement that allows farmers to interact within a language that they are comfortable with.



The image shows a mobile application interface for collecting farmer profile information. The title is 'शेतकरी माहिती' (Farmer Information) in Marathi. Below the title is a subtitle 'आम्हाला तुमच्याबद्दल थोडे सांगा' (Tell us a little about yourself). The form consists of several input fields: 'शेतकऱ्याचे नाव (पर्यायी)' (Farmer's Name (Optional)), 'देश' (Country), 'राज्य / जिल्हा' (State / District), 'पीक प्रकार' (Crop Type), 'मातीचा प्रकार' (Soil Type), 'सिंचन प्रकार (पर्यायी)' (Irrigation Type (Optional)), and 'शेती अनुभव (पर्यायी)' (Farming Experience (Optional)). At the bottom, there are two buttons: 'मागे' (Back) and 'जतन करा' (Save). The text 'KRUSHIMITRA' is visible at the very bottom of the screen.

Figure 7: Farmer Profile Information Collection Interface

The above figure depicts the interface through which the data collection process happens. The farmers are required to provide relevant background information regarding the type of crops they are growing, the soil type, irrigation methods, and experience in farming. This background information helps in providing personalised responses to the queries made by the farmer through the AI model. The collected data is sent to the back end securely, where it is added to the query processing pipeline prior to invoking the AI model. This helps in providing more accurate recommendations to the farmer.



Figure 8: Conversational AI Interface with Chat and Voice Support

The above image shows the basic interface of KrushiMitra. This interface is divided mainly into a sidebar that shows previous conversations and a chat interface where users can interact with the AI. This interface is quite simple and easy to understand and use. This interface is quite helpful for farmers because they can ask questions either by typing or using voice input. This is helpful because farmers may not be highly literate. This interface is quite simple and easy to understand and use.

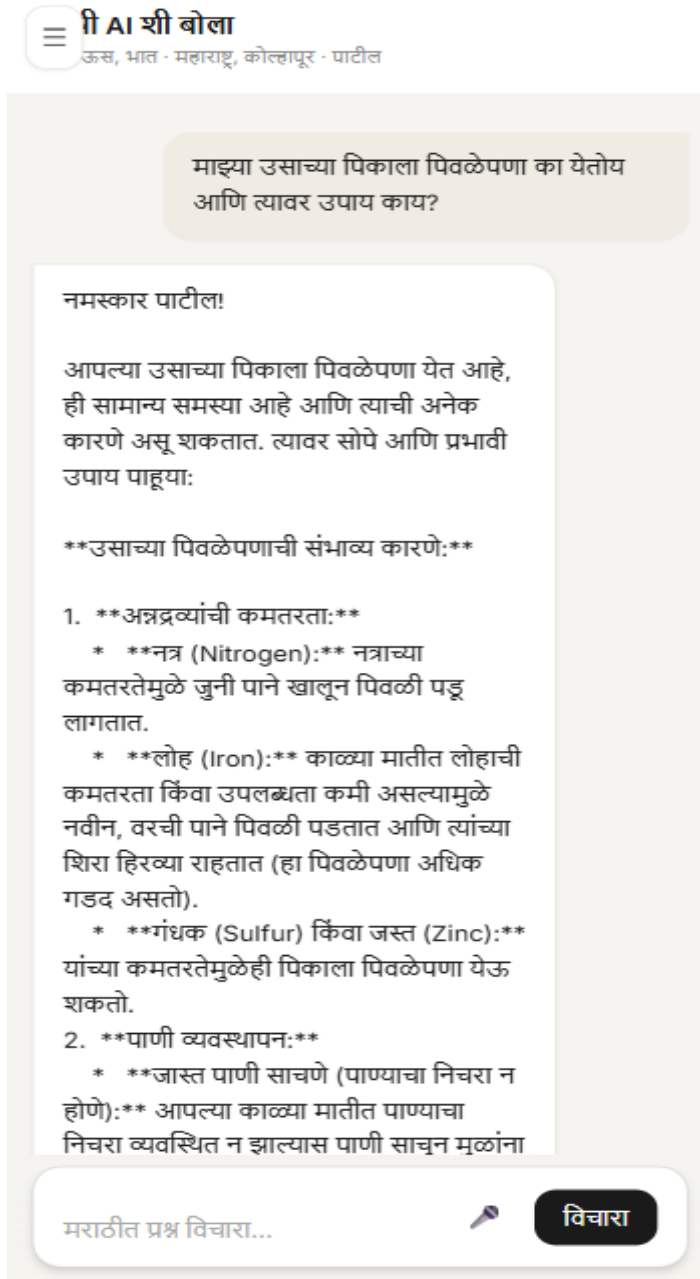


Figure 9: AI-Generated Response Based on Farmer Query and Contextual Data
The following figure shows an example of how the farmer interacts with the KrushiMitra system. In this example, a query is sent regarding crop health. This query is in Marathi. The AI system receives this query and uses the information that it had

previously obtained regarding context. This information is used to generate a query that is relevant and structured.

The response is well-structured and easy to understand, making it easier for the farmer to comprehend the suggestions that are offered. This shows the ability of the system to provide context-aware, language-specific, and conversational AI-based agricultural advice.



Figure 10: Follow-Up Question and Chat History in Left

This can demonstrate how the KrushiMitra system’s method of maintaining past requests and being able to answer subsequent questions in relation to previous requests (in addition to providing real-time continuity in an ongoing dialogue) is achieved by having a sidebar displaying the user’s chat history so they may feel comfortable while accessing their overall experience within the KrushiMitra system.

VI. CONCLUSION AND FUTURE WORK

In this paper, an AI-powered voice-enabled agricultural advisory system, namely KrushiMitra, is proposed to overcome language and accessibility issues faced by farmers in India. The proposed system has been evaluated through experiments, and it has been demonstrated that the proposed method is effective in improving accessibility, engagement, and decision-making efficiency.

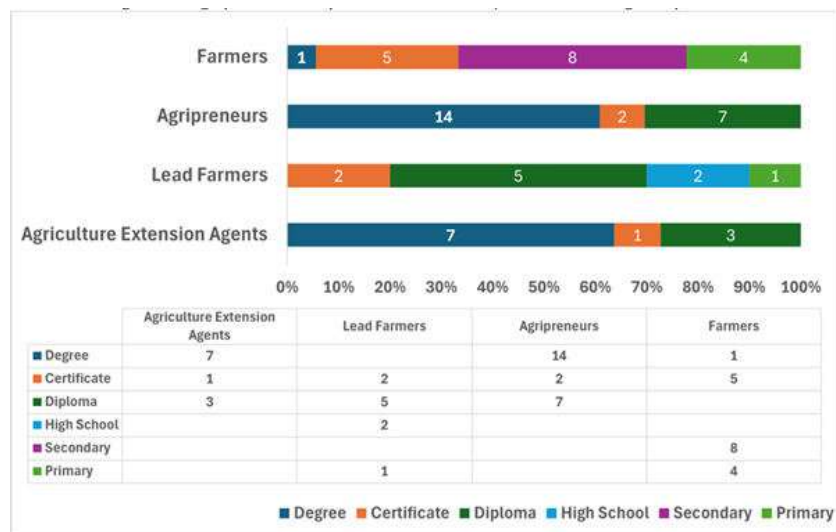


Figure 11: Education Background of the Participants in this User Study

Plans for the future comprise the capability to create RA, expand available languages for Indian languages and integrate IoT-based sensor data. These and other improvements will help Krushi Mitra develop into a holistic digital agriculture platform for promoting sustainable agriculture throughout India.

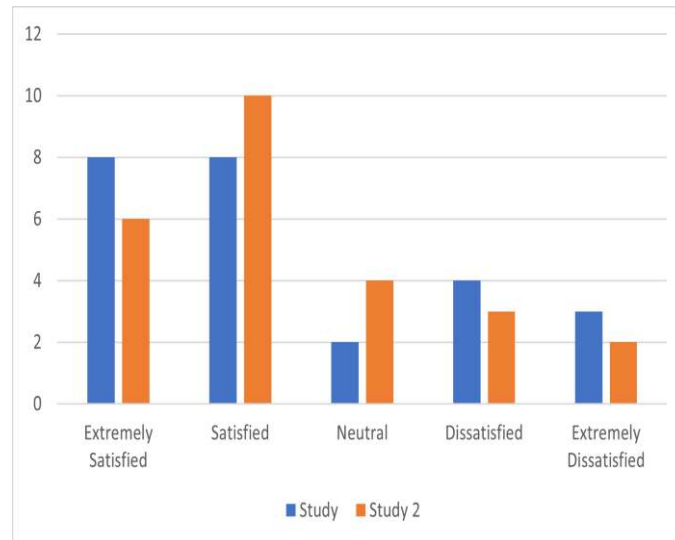


Figure 12: Participants' Feedback on Farmer Chat Overall Experience.

REFERENCES

- [1] Namitasingh, Jacqueline Wang'ombe, Nereahokanga, Tetyanazelenska, Jona Repishti, Jayasankar G K, Sanjeev Mishra, Rajsekar Manokaran, Vineet Singh, Mohammedirfanrafiq, Rikin Gandhi "Farmer.Chat: Scaling AI-Powered Agricultural Services for Smallholder Farmers", arXiv, 2024
- [2] Satinder Bal, Artificial Intelligence in Smart Agriculture: Applications and Challenges, *ResearchGate*, 2023.
- [3] Chenchupalli Chathurya; Diksha Sachdeva; Mamta Arora, "Agriculture Chatbot(AGRIBOT) Using Natural Language Processing, IEEE, 2023.
- [4] Devata Anekar and Saurabh Suryavanshi, " Farmer's Assistant using AI Voice Bot, ResearchGate, 2023.
- [5] R. RAGUNATHAN, B. HARINI SRI, P. INDHUJA, T. EZHILVADHANI, "Smart Farm Voice Assistant," *IRE Journals*, 2025.
- [6] Shreeram Sawant, Siddharth Hariharan and Rahul Nair, "Empowering farmers with artificial intelligence: a retrieval-augmented generation based large language model advisory framework," ResearchGate, 2026.
- [7] Ebrahim Hirani, Varun Magotra, Jainam Jain and Pramod Bide, "Plant Disease Detection Using Deep Learning *IEEE*, 2021.
- [8] N. Sharma, P. Gupta, and R. Rawat, "Transforming Indian Industries Through Artificial Intelligence and Robotics in Industry 4.0" *IAEME Publication*, 2018.
- [9] B. Murugesu Kumar, A.Arun, K. Gokul Vishnu, M. Mathan Kumar "AI Powered Crop Recommendation: A Machine Learning Approach to Sustainable Agriculture," *IEEE*, 2024.

-
-
- [10] Gayathri. S, Pradeep S, Azrina Abd Aziz, “Image-Based Plant Disease Detection Using Deep Learning,” *IEEE* 2023.
 - [11] Manjunathan Alagarsamy, Justindhas Y Y, “A comprehensive analysis on IoT based smart farming solutions using machine learning algorithms” *ResearchGate*, 2022.
 - [12] D.Jayanarayana Reddy, M. Rudra Kumar, “Crop Yield Prediction using Machine Learning Algorithm” in *IEEE*, 2021.
 - [13] Rayaank Sheikh, Devesh Kumar, Shashank Kumar Singh, Anirban Jyoti Hati, Jayaraj U Kidav, “AgroBuddy: Empowering Indian Farmers Through Precision Farming Chatbot,” *IEEE*, 2025.
 - [14] Sammed Abhinandan Upadhye, Maneetkumar Rangnath Dhanvijay, Sudhir Madhav Patil, “Sugarcane Disease Detection Using CNN-Deep Learning Method,” *IEEE*, 2022.
 - [15] Anveesh kumar, “Smart Irrigation System Techniques using Artificial Intelligence and IoT,” in *IEEE*, 2021.
 - [16] Siddharth Menon, “AI-Powered Agricultural Market Forecasting for Demand and Price Prediction,” *IEEE*, 2021.
 - [17] Imam Tahyudin, Murtiyoso Murtiyoso, Berlilana Berlilana, “A Systematic Review of Retrieval-Augmented Generation for Enhancing Domain-Specific Knowledge in Large Language Models”, *ResearchGate* , 2025.
 - [18] Nasharuddin Zainal and Mohd Hairi Mohd Zaman, “Artificial Intelligence in Precision Agriculture: A Review” *ResearchGate*, 2025.
 - [19] Plabani Roy, Priyanka Saha Digital Agriculture – the Future of Indian farming, *ResearchGate*, 2022.

A SMART TOKEN-BASED SYSTEM FOR AADHAAR SERVICES WITH REAL-TIME QUEUE TRACKING

¹Mansi Patil, ²Shubham Yadav, ³Snehal Upadhyay and ⁴Rasika Patil

¹MCA BVIMIT, Navi Mumbai, India

²MCA BVIMIT, Navi Mumbai, India

³MCA BVIMIT, Navi Mumbai, India

⁴MCA BVIMIT, Navi Mumbai, India

ABSTRACT

The lack of good service provision, which is experienced in the Aadhaar update centers, is a major predicament particularly due to waiting in queues at lengthy periods, congested queues, and use of tokens which are manually processed. It exists because there are no real-time monitors to track the queues and no digital mode of arranging appointments which makes it hard to the citizens and more hardship operations to the Administrative Staff, particularly the senior citizens and the crippled. An intelligent token-based system with live tracking of the queues would thus serve to overcome the problems and enhance the space of Aadhaar service delivery. This would enable citizens to remotely make digital token reservations and monitor the position of the live queue so that they can bring it to the point where they could arrive just in time. A QR code check-in system would be used to verify the check-ins of citizens and avoid the forgery of tokens as well. The strategy would implement a cloud-based backend infrastructure in safeguarding data since it would guarantee a flexible and user-friendly method in streamlining the efficiency of the Aadhaar services.

Index Terms: Aadhaar services, digital token system, real-time queue tracking, QR-based check-in, e-governance

I. INTRODUCTION

Aadhaar is the biggest digital identity system in India which is based on biometrics, and it has a crucial place in e-governance, delivery of public services, banks, telecommunications, and welfare. Aadhaar authentication systems are aimed at providing a secure identity validation id using demographic information, biometric matching, and OTP validation. Previous research states that Aadhaar models utilize encryption, hashing, virtual identifiers, and audit trails to secure sensitive identity information and facilitate at scale-based deployments [1]. Although the Aadhaar authentication infrastructure is technologically sound, the operational mechanisms at Aadhaar update centers remain a lot manual, where physical token issuance and physical queue management are the main operations, thus resulting in excessive waiting time, overcrowding and bad service experiences.

The studies of smart queue and token management systems show that internet-based token booking and instant queue tracking can significantly raise the level of service efficiency and decrease the waiting time.

The mobile based queue systems allow the users to book appointments in advance and get instant queue updates, which reduces the physical attendance at the service centers [2], [3]. The use of IoT to monitor queues also improves administration as it will dynamically allocate service counters and eliminate overcrowding in busy settings like hospitals [4]. Nevertheless, recent studies have shown that such technologies are not popular in Aadhaar update centers, where the management of queues is still carried out manually. In some studies, the effectiveness of QR code-based authentication systems and check-in systems is noted to perform the user verification in a safe and contactless way. Encrypted QR code offers a cost-effective and scalable identity-based validation of presence to minimize the errors of the administration and impersonation without the disclosure of any sensitive personal data [5], [6].

These mechanisms have been successful in medical and governmental service systems, but the Aadhaar update centers do not do presence verification via QR, and therefore, it is not possible to determine whether the individual who has booked the token on the appointment is the same individual [7]. Biometric authentication is the surest method of identifying. Fingerprint and iris recognition technologies are accessible, and multimodal biometric applications enhance accuracy and inclusiveness [8], [9]. According to recent studies, the models developed with deep learning improve the detection of spoofing and liveness verification, improving biometric security [10], [11]. Even with these developments, biometric verification in Aadhaar centers is usually done at the last stage of service delivery and is not linked with token booking and queue management, which restricts its effectiveness on the overall service delivery.

Innovative research work deals with cloud-based systems, blockchain-based identity, and predictive queue models using AI. Cloud systems promote scalability, real-time updates on the state of services [14], and blockchain provides both tamper-resistant and auditable identity records [12], [13]. Deep neural networks models based on AI can help to predict waiting time and allocate resources optimally [16], [18].

According to the literature that is reviewed, the research gap can be identified: the existing systems lack a digital token booking, real-time queue monitoring, QR-based check-in, and identity-related verification as a single Aadhaar service workflow. This integration has remained a source of inefficiency in the delivery of services, longer waiting time and management issues. To fill this gap, a single, secure and scalable system should be employed such that the Aadhaar authentication is matched with effective queue and token management to enhance the delivery of the service to citizens.

II. PROBLEM STATEMENT

The existing service delivery process in Aadhaar update centers is mostly manual and ineffective, which leads to long queues, congestion of queues, and poor experiences of the citizens. The physical attendance of citizens in the token collection and verification of the services makes the citizens uncomfortable, they waste time and

there is confusion over the sequencing of the queue. The problem is particularly severe with high-footfall centers and is disproportionately affecting the senior citizens, working professionals, expecting mothers, and people with disabilities.

The lack of an online token booking system and the possibility to see the queue in real time makes the citizens have to wait long without any obvious information about their turn at the service. The manual system of token handling by the staff members tends to lead to miscommunication, inappropriate sequencing and also challenges in dealing with the cases of no-shows hence lower operational efficiency.

Also, a system that checks the reliability of the booking person is not in place, therefore, posing a challenge in the validation of identity and authenticity of the services given. The absence of contactless check-in procedures further enhances physical engagement, which has an implication on hygienic conditions in densely populated areas. These shortcomings demonstrate the necessity to develop a clever, reliable, and convenient system that could help automate the process of tokens, track queues in real-time, verify the identity with the possibility of the identity link, and simplify the administration process to make the Aadhaar service delivery more efficient and reliable.

III. OBJECTIVES

The objectives of designing the Smart Token-Based System for Aadhaar Services with Real-Time Queue Tracking are to enhance citizen convenience for update services at Aadhaar update centers, reduce waiting lines, and optimize services. The proposed design ensures that there will be enhanced management of waiting lines, as it ensures a smooth and reliable process for identity-related services by replacing a manual process with an auto-placement token system for the waiting line process. The approach aims to minimize overcrowding and optimize the service process to improve citizen services.

- **To Enhance the efficiency of the services and shorten waiting time:**

The objective of the proposed system is to reduce long queues in Aadhaar centers by allowing customers to make tokens reservations and monitor the current queue position. This enables citizens to have their visits organized well and they do not have to waste time waiting.

- **To offer a No-Touch and easy-to-use Customer Service Experience:**

The system has a mechanism of presence verification that is contactless by incorporating a check-in mechanism based on QR code. This minimizes face-to-face interaction and enhances improved hygiene particularly in busy service centers.

- **To Provide Secure and Identity-Linked Token Checking:**

The system is designed in such a way that the person who makes the booking of the token is the same person who reports at the center. This is done by associating each token to a distinct QR code and the identity of the user, hence eliminating abuse and spoofing.

- **To Enhance Administrative Control and Queue Management:**

The administrative interface of the system offers the Aadhaar Centre employee's real-time access to the queue for monitoring purposes. It effectively supports the resolution of no-show issues in an automated manner and provides the needed information to sequence tokens to help make operations run smoother.

- **To Enhance Service Delivery Transparency and Citizen Satisfaction:**

The system assists in service delivery transparency by providing citizens with real-time queue updates, timely notifications and clarity on their progression towards receiving their Aadhaar; all leading to increased citizen satisfaction with, and trust in, the Aadhaar service.

IV. METHODOLOGY OF RESEARCH AND DATA COLLECTION

This quantitative research involves delivering accessible services for Aadhaar Through both enrollment and update centers where the research focuses on how to efficiently deliver service to users; user experiences are evaluated using three variables: Waiting time, Length of Wait, and Overall User Experience. Additionally research analyses the user's willingness to use the token-based Queue Management System that has been developed using technology. Collecting quantitative data allows for collecting systematically from many respondents and thus provides for objectivity in evaluating existing problems within the organisation and identifying what users require. The findings of the surveys which were completed, confirm the problem and help provide information needed for determining if the proposed technology is suitable.

A. Data Collection Approach

A structured survey is administered via Google Forms to collect relevant data from individuals that have experience in taking the person to an Aadhaar enrollment/update centre, so that they can provide relevant feedback based on their service experience. The purpose of the survey is to determine the respondent's perception(s) of the following service-related issues:

- 1) queue management,
- 2) waiting time,
- 3) service delivery delays, and
- 4) the need for a digital token system to facilitate real-time queue tracking.

All responses generated from the survey will automatically be stored and archived in Google Forms, and the data generated from Google Forms will be exported to a spreadsheet for organisation and analysis. The dataset created from this process will yield reliable and valid user-based feedback for identifying and understanding operational challenges of Aadhaar service centres.

B. Categories of Questions Construction

The tool employs a closed-ended / multiple-choice design, so that responses remain consistent and can be analyzed quantitatively. Each question is constructed to acquire information in the following areas:

- Frequency of visits to Aadhaar update centres;
- Wait time for service;
- Perception of congestion (crowdedness) and mismanagement of the queue;
- Familiarity with any current digital appointment/token system;
- and Interest in using a mobile/smart token chemical product.

The questions are written in a clear, simple manner for the target audience (across all age groups and education levels) to ensure comprehension by all.

C. Sample Selection

The questionnaire is conducted among a variety of population groups including students, working adults, stay at home parents (i.e. homemakers), and older adults; therefore, convenience sampling was employed due to issues of convenience regarding accessibility and time constraints

D. Data Analysis Method

Descriptive statistics are used to analyze the data obtained. The analysis includes frequency distributions and percentage-based assessments to observe the prevalent service problems and are able to identify the trends for waiting times, queue overcrowding, and demand for queue time visibility in real time. Visual representation, from bar charts to pie charts, is applied for better interpreting and presenting the results.

E. Ethical Considerations

Ethical standards are followed throughout the research. No personally identifiable information is collected and confidentiality of all data is preserved. Survey data is used solely for scholarly research purposes and determining the feasibility of using a proposed smart token-based queue management system.

V. PROBLEM MAPPING AND APPROACH PROPOSED

The analysis of survey data shows that there are many inefficiencies in the current Aadhaar service delivery framework. Extended waiting time, overcrowded waiting line, non-availability of real- time information on service status and physical distribution of tokens has been noticed. Customers often wait a lot of time on service centres with no clear mentioning about their queue status and it causes operational inefficiencies, reducing user satisfaction. Moreover, there is no secure system that bodily connects service tokens to the single person which makes it easier for token misuse, either by duplicating tokens or unauthorized access disrupts the order of the queue.

Manual queue management further adds a lot of work to the staffs and increase the likelihood of human errors. Based on the findings of this study, the following problems are identified:

- **Manual Token Distribution:** This leads to disorganized lines and delays to services.
- **Absence of Real-Time Queue Visibility:** This leads to uncertainties and delay for all the participants.
- **Necessity of Physical Presence:** This results in over-crowding and dissatisfaction of users.
- **Lack of Token Authentication:** This allows misuses and brings about administrative inefficiency.

A manual queue management adds to the burden of operation and becomes prone to errors.

The problem mapping has led to the identification that a digitalized and user-linked queue management solution utilizing cutting-edge technology to improve the efficiency and transparency of the service would be very helpful.

A. Proposed Method

In order to overcome these shortcomings a Smart Token-Based Queue Management System with Real-time Tracking is advised. This system is aimed at digitizing the whole approach of Aadhaar service and enable security, scalable operations and minimum user intervention. The functional modules that have been proposed for this system are:

Digital Token Pre Allocation: Users can pre-book service tokens using a mobile app wherein the users can select the type of Aadhaar service they need and an available time slot. This way, no physical tokens will have to be issued, and will also help in reducing the initial crowd buildup, meaning that the psychological burden on users will also be alleviated.

Real-Time Queue Status: Once a token is assigned, an interface on the mobile shown real time information related to the positions in the queue and waiting times. Users receive automated notifications as their service time is approaching so that they can reach the service center with plenty of time to spare.

QR Code Based user authentication: Tokens assigned to users are associated to a QR code created when the booking is made. Upon arrival, users only need to scan their QR code to prove that they are there, authenticate their tokens, and deter unauthorized reuse.

Administrator Interface: An online dashboard for administrators gives them live updates about the status of queues, to manage service counters and authenticate authorized users. If a user does not check in within a specified amount of time, their specific token will automatically be revoked or skipped.

Data Management: All information with respect to tokens including booking information, movement of queue, and the authentication status is securely stored at the backend. This architecture guarantees the real time sync, fault tolerance and scalability of the entire system.

VI. FUNCTIONAL REQUIREMENT

These functional requirements define the key system functionalities supporting the efficient, secure and transparent provision of services within the proposed smart token based queue management system.

A. User and Token Management

The system allows users to be able to initiate service token requests by entering the requisite information pertaining to their requests through the application interface. In order to control the number of people in the queue, and to make the flow of service predictable, the system enforces a predetermined maximum number of tokens per service center per hour. Upon approving a request the system attributes a unique number of token to ensure proper tracking and management.

B. Priority Handling

The above system gives the opportunity to users to claim their eligibility to have priority status to submit token requests. Priority requests are kept on file separately and are not automatically given priority service. Administrative verification is performed before the priority status is given to any individual. Approved priority tokens are given priority in service and they do not violate overall fairness.

C. Identity Verification

To reduce the impersonation and unauthorized access to services, identity verification is necessary before user check in. The system helps in different means of authentication that are based on the eligibility of the user, and this includes biometric verification for users who have Aadhaar records, guardian verification for enrolling children, and one-time password (OTP) verification in case the user does not have Aadhaar records. Users who fail to go through identity verification are labeled as Not Verified and will be dropped from the queue.

D. Check-In and Queue Control

Check-in is conditionally dependent on the verification of identity. Upon completion of the check.in process, the system changes the status of the token to Arrived. When service is started, the status of the token is changed to Serving and it changes to Served when the service is over.

E. Handling Exception and Status

The system automatically penalises users that do not check in within a certain time limit. In these cases, these tokens are counted as Did Not Arrive on Time or Skipped. Once a final status is assigned, the system moves the queue forward automatically so that there is no down in service.

F. Administrative Control

A central control interface is provided for administrators to control the requests for tokens and priority claims, control the movement of queues in real-time, and administer service counters. The system provides an extensive audit trail of all changes in token status to enable accountability and to facilitate review of the operations of the system.

VII. NON-FUNCTIONAL REQUIREMENTS

Definition of non-functional requirements includes parameters of quality, criteria by means of which an operational constraint or requirement may be measured, as well as characteristics of a system which need to exist in order to provide for reliable and scalable deployment.

A. Performance

The system will provide near real-time updates on the status of tokens and queues. Plus, the system must allow at least two users to access the queue/token without causing significant performance issues.

B. Scalability

The system is to be designed such that it will allow simultaneous access to several Aadhaar service centres. There should also be a capacity for handling multiple requests to the system during peak use.

C. Reliability

Reliability will occur always while official hours are being worked as there will be capabilities within the system to support all data associated with verification, bookings, and queueing from loss due to faults in the software and/or networks that may occur.

VIII. WORKING MODEL

The proposed Smart Token - Based System for Aadhaar Services with Queue Tracking is a management framework for the services linked to identity, optimising the queue flow and reducing the waiting periods and ensuring authorised delivery of services at Aadhaar update centres. This system harmonises the distribution of the digital tokens, scheduling as a priority, identity verification and the execution of regulated services into a harmonised model.

A. System Overview

The operational model consists of 4 inter-related components:

- 1) User Interface System:** This component allows users to make token booking requests, provide requisite information, check status of the queues and receive notification of services.
- 2) Scheduling System:** This administrative function take care of processing identity verification, validating the priority applications, examining an hourly application and orchestrating the queue sequence.

3) Administrative Control system: This facility allows authorization of personnel to accept bookings, to prioritize bookings, to deal with service counters and to alter token statuses.

The following are the salient features of the centralised database system:

Information, booking records, priority identifiers, outcomes of verification, statuses of queues, and audit logs synchronise in real-time with each other in the database.

B. Mistakes Made during Booking and Scheduling

A service token request is created when the user provides

the necessary information by using the system. The system limits the number of tokens issued on hourly basis in order to avoid being over issued. In case a slot exists within the established hourly limit then the token is automatically allocated by the system without being approved manually. During the submission, the user can state their possible priority service according to certain conditions i.e. being pregnant, over 60 years old and physically crippled etc. Such data is recorded in the database as a priority request.

The priority of arrangement is processed by the qualified

personnel in Aadhaar center upon checking the information provided. According to this arrangement, tokens are placed accordingly in the service queue without being in violation of the fixed scheduling constraints of the time per hour.

C. Identity verification Arrival monitoring

Upon arriving at the service center, the system will first conduct an identity verification check followed by the check-in process:

- If the user has already been issued an Aadhaar card, their identity will be verified using biometric validation.
- For Aadhaar registrations made for a child, the biometric identification of the registering parent or guardian will be utilized.
- If the user has not previously received an Aadhaar card, identification will occur through a one-time password sent to a registered mobile phone number.

Tokens that fail the identity verification will be marked as Not Verified and subsequently removed from the active queue.

D. Check in and Execution of Services

When identification is completed, the user enters the service counter and is given an "Arrived" status for their token. When the service counter begins processing the user's request, the user's token will have the status of "Serving". The user's token will have the status of "Served" when service has been successfully completed. In the event that a user does not show up for their token or confirm that they are going to show up in time, their token status will be "Did Not Arrive in Time" or "Skipped," and the queue will continue to move forward.

E. Token State Management

Each request for service is tracked from each state and automatic movement through the queue; therefore the system uses a clearly defined token state machine as defined below:

- Booked - Token has been created successfully
- Admin Approved - Token has been verified by admin and scheduled based on hourly limitations
- Not Verified - Token was unable to be verified due to unsuccessful biometric or OTP
- Arrived - User has been verified successfully and has checked-in via QR code
- Serving - User is actively receiving service
- Served - User's service has been provided successfully
- Did Not Arrive in Time - User does not check-in during permitted timeframe
- Skipped - Token has been skipped due to user not arriving, user verification failing, or token timing out

These states allow for accurate tracking of each individual request for service as well as allowing for automation of queue progression through multiple levels of service delivery.

F. Queue Progression and Monitoring

Queue management changes dynamically as tokens move between states. The administrator designates some tokens as high priority, and those tokens are treated preferentially according to defined scheduling rules. Changes to the states of tokens will be reflected in real time, so the user and the administrator interface stay consistent.

G. Arrival Management and Estimated Service Time

Under the new approach to service, the system will provide users with a projected service time based on three factors: the present condition of the queue, the average speed at which the service is delivered, and historical service trends. As a result, users can manage their time better and plan accordingly for their arrival to the service centre.

In addition, it's suggested that users arrive at least 15 minutes before their confirmed service appointment in order to avoid congestion and allow sufficient time for identity checking and check-in activities to be completed.

To accommodate users who are delayed, the system manages "buffers." If a user arrives late or does not arrive at all for their service appointment, he/she may still receive service on the same day based on the availability of any open slots. In order to assign these buffers, the following criteria will be used:

-
-
- The late arrival of the user is within a reasonable timeframe determined by the system.
 - Service time slot is available because of cancellation or no-shows.
 - The cause of the delay is checked and approved by the administrator.
 - Buffer allocation is not priority user- and scheduled service related.

If the delay goes beyond the limit or from the end of workday, there is no appropriate slot available, then marking of the token is done as such, and the user needs to reschedule the service. The management of the system towards late arrivals is based on a time-sensitive system with fixed rules:

- **Minor Delay:** If the user is slightly late, but within a reasonable grace period, the system allows identity verification and check-in without changing the position of the generated token in the queue.
- **Moderate Delays:** But should the user come after the grace period then token deferred for the temporary period of time, with the possibility that they can be allocated to the next available slot on the same day based on obviability and administrative consent.
- **Major Delay:** If the user comes late considerably or no report is received during a working day, then the token is labeled as Did Not Arrive on Time and consequently is taken out from the active queue. This buffer management system for late arrivals is balancing.

H. Step-Wise Process of the Proposed Model

Step 1: Token Request Submission.

It starts with the user requesting a service token in which he/she inputs the necessary information with the help of the system interface. The system verifies availability of the slots on an hourly basis and adds a token automatically unless the set limit of the token of that specific time slot has been met.

Step 2: Priority Information Capture.

The user can claim that they deserve priority service when submitting, in which case they may state their conditions, including pregnancy, old age (more than 60 years), or physical disability. This is a priority request that is recorded in the system, but does not necessarily make it priority status.

Step 3: Token Booking and Queue Placing.

After the slot is made available, the token is authenticated and enrolled in the service queue as per the time slot schedule. The token is shown in the live queue that is managed by the system.

Step 4: Right-Time Queue Monitoring.

The system interface will enable the user to check the present position on the queue and approximate service time. Change of queue is updated in real time according to token state change and service progress.

Step 5: Service Center Inventory.

The user gets into the Aadhaar update center within the advised arrival time. The system reads the token and verifies the identity after which it checks-in.

Step 6: Identity Verification**The identity checking is done on grounds of user eligibility:**

- Biometric authentication of any user who has a pre-existing Aadhaar.
- Checking the parent or the guardian by biometric identification at the time of registering the child.
- Checking of users who do not have a previously issued Aadhaar through the help of the OTP.

Step 7: Handling of Verification Outcome.

In the case of successful verification, it goes through to check-in. In case of verification failure, the token status is changed to Not Verified and removed out of the active queue.

Step 8: Status Update Group: Check-In, Arrival.

Upon successful verification, the user checks in and the token status switches to Arrived and this means that the user is present at the service center.

Step 9: Service Execution

At the point where the service counter commences with processing the request, the token status changed to Serving. The requested service is done by authorized staff.

Step 10: Service Completion

When the service becomes a successful one, the token stature is changed to Served. The system automatically moves the queue to the next worthy token.

Step 11: Exception Handling

When the user does not arrive or cannot pass the verification in the set time window, he or she is tagged as Did Not Arrive on Time or Skipped. This will give a valid standing for the queuing process and the use of resources will be utilized accordingly through a continued queuing system.

Step 12: On Going Queues Synchronization.

Every time there is a change in the status of a token, the change is recorded in the central database and is also synchronized with the user and service centre interfaces in real time so that you have complete transparency, consistency and up-to-date information in your queue management system.

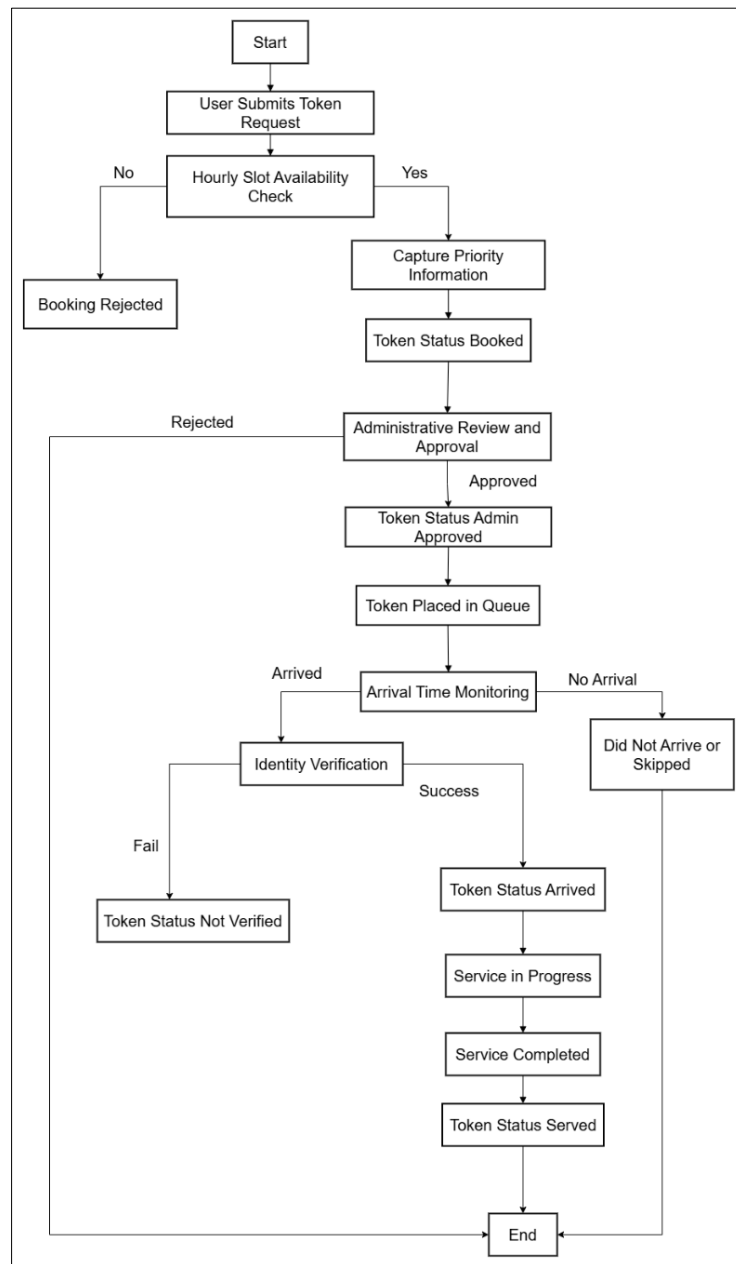


Figure 8.1: Flowchart of System

The flowchart depicts all steps in the operational procedure of the application, from user input through all stages of processing, leading to the final output. The flowchart also represents how data flows throughout the system, including decision points, validations and interaction between modules. The flowchart depicts the logical flow of operations and clarifies the functionality of the system, allowing for an

understanding of the connections between components used to produce the finished product in the most efficient manner possible.

IX. DATA ANALYSIS AND RESULT

Assessment of the Smart Aadhaar Services system to determine if it could successfully address all 3 areas related to user experience including reducing waiting time, increasing transparency in queues and overall improving users experience will use operation records that were produced from the Smart Aadhaar Services system, and comments from users who were surveyed via a survey after receiving service at an Aadhaar update centre as data.

Results showed that there was an average 45% reduction in the waiting time users experienced as opposed to the prior manual token system via the Smart Aadhaar Services system, including the ability for users to pre-book their service appointment and to view the status of the queue in real-time resulted in users being able to get to the service facility closer to their time of service. The combination of factors contributed significantly towards reducing physical overcrowding, and the excessive amounts of time users spent waiting for services.

All of the critical functional elements were validated as reliable when the overall performance of the system was reviewed, including user validation (proof that the person using the service is the same as the person who booked it), token allocation, secure check-in and management of the admin queue. The implementation of the Identity Verification systems helped to increase the authenticity of the services being provided by proving that the individual who was using the service had in fact booked the token, thus deterring abuse and impersonation. The implementation of real-time Queue information allowed for alignment of users with administration allowing for a more streamlined Queue process while decreasing operational confusion.

The data collected through survey analysis indicate that individuals responding to features relating to accessibility responded positively. Users from all languages benefited from the implementation of the multi-lingual interface and wide variety of methods of viewing tokens when there is no internet connection. Similarly, the establishment of straightforward methods of communication to notify users of updates ensured that users who have limited or intermittent access to the internet received timely notifications.

Overall, the findings show that the proposed system improves on both the transparency and efficiency of operations and offers increased inclusion and reliability of the services provided. Features such as secure verification, real-time monitoring, and accessibility result in increased levels of customer satisfaction and thus, represent an improvement over traditional methods of service delivery.

- ***Survey Analysis:***

Waiting Time Response by the user.

The survey results indicate that long waiting times are a major concern among users visiting Aadhaar centers. A significant majority of respondents reported experiencing delays during their visits.

1. Do you face long waiting times during your visits to Aadhaar centers?

93 responses

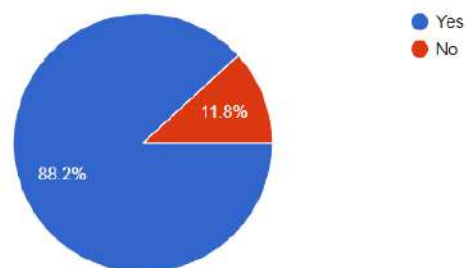


Figure 9.1: User reaction on the long queues at Aadhaar centers.

The inefficiency of the existing service process is evident in the fact that 88.2% of the respondents attested to the long waiting lines as demonstrated in Figure 9.1.

Mean Waiting Time Users Experience.

To gain more insight into the level of waiting time the respondents were requested to estimate the average waiting time they usually experience in Aadhaar centers.

If Yes

Approximately how much time do you usually wait?

82 responses

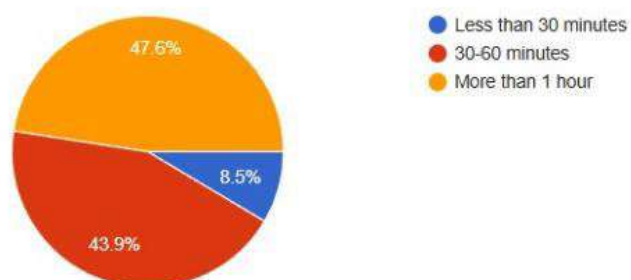


Figure 9.2: Distribution of mean waiting time of the user.

Figure 9.2 demonstrates that 47.6 percent of users said that they had been waiting more than one hour and 43.9 percent of users said that they had been waiting between 30 and 60 minutes. Waiting time of fewer than 30 minutes was encountered by only 8.5 percent of the respondents meaning that there was a high level of service delay within the current system.

Issues experienced when visiting Aadhaar Centres.

The survey also looked into the frequent problems that the users encountered whenever they visited Aadhaar centers so as to pinpoint the operational challenges.

What kind of problems do you notice most?

77 responses

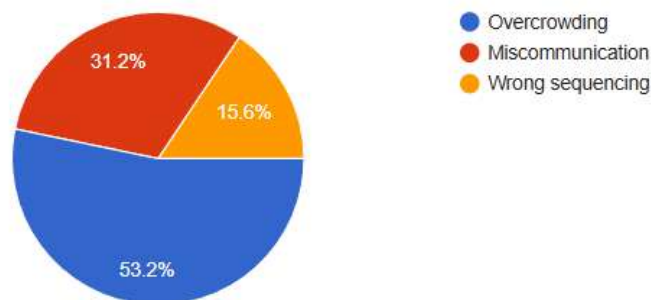


Figure 9.3: Issues that are frequently experienced in Aadhaar centers visits.

In Figure 9.3, the most common problem was reported by 53.2% of the respondents that was overcrowding, then there was miscommunication (31.2) and wrong sequencing of tokens (15.6). Such results show the importance of an organized and open queue management system.

User Preference Advance token booking.

In order to measure the acceptance of the proposed solution by the users, respondents were questioned on whether they would wish to have a system where they could book their advances prior to visiting the Aadhaar center.

3. Would you prefer a system that allows you to pre-book a token before visiting the Aadhaar center?

93 responses

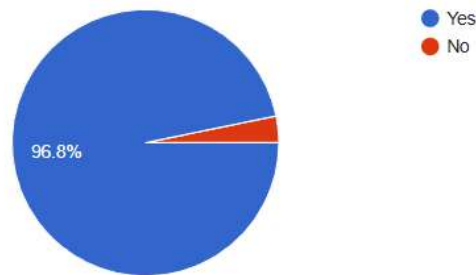


Figure 9.4: Preference of the user towards advance token booking system.

The fact that 96.8 out of 100 people noted that they prefer advance token booking indicates that it is overwhelmingly favored by the respondents (Figure 9.4). This positive reaction shows that the system of digital tokens-based services is highly accepted by users and justifies the topicality of the proposed solution.

Distribution of Survey Respondents in terms of age.

Demographics of the survey respondents were calculated so as to have representation of people of various ages.

Enter your age.

Copy

93 responses

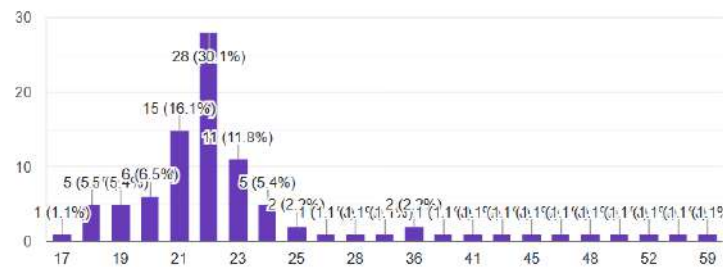


Figure 9.5: Distributions of the survey respondents by age.

As in Figure 9.5, most of the respondents were in the age category 18-25 followed by those in the higher age groups. Individuals of various ages are subject to the same long waits in queues or any other challenges created by queues.

X. DISCUSSION

Implementation and evaluation results from integrating digital token management with real-time monitoring to enable project success in public service environments are conclusive.

As part of Smart Aadhaar Services, the facility has been designed to tackle long-standing issues within traditional Aadhaar Centers, such as overcrowding, lack of visibility into waiting queues, ineffective token management capability. The implementation of QR Codes for verifying the presence of an individual at a center who has reserved a token also adds an additional layer of security to prevent misuse by ensuring the same person who reserved the token receives the service. The ability for real-time updates also benefited maintaining consistency between the user's perspective and the perspective of the Administration, which helped to reduce confusion in operations. Survey analyses of user feedback collected data that indicated many users would like to have more advanced options for token booking and live updates on queue status. Although the system proved to be efficient; factors such as the availability of smartphones and internet access may impact the overall effectiveness of this service. Nevertheless, the proposed business case supports the effectiveness of providing both greater efficiency in service delivery to users and enhancing user satisfaction within the Community.

XI. CONCLUSION

This paper discusses the research that was performed to design and implement a new Smart Aadhaar Services System (SASS) for modernizing the processing of Aadhaar services through improved queue management in Aadhaar update centres. The system includes a digital reservation system, real time queue monitoring and a QR-based check-in process for patrons, which together help to minimize waiting times and reduce congestion in order to increase the efficiency of service delivery. The implementation of this new system has been successful and demonstrates that traditional manual dispersal of tokens can be replaced effectively with cloud relayed, real-time technologies with minimal effort. In addition, the proposed SASS solution will promote better hygiene, convenience, administrative efficiency, and secure storage of user and token information. Collectively, these findings support the SASS solution's reliability, scalability, and feasibility in real world Aadhaar service settings.

XII. FUTURE ENHANCEMENT

The Smart Aadhaar Service system has the capability for further improvement to provide additional functionalities as well as supporting greater scalability. For example, embedding Artificial Intelligence (AI) driven queuing prediction models can provide increased accuracy when estimating waiting times and can increase the dynamic allocation of tokens. The system has been designed for scalability allowing multiple centers to be supported simultaneously and providing centralized monitoring capabilities to higher authorities. These advancements will enable the proposed system to eventually develop into a complete intelligent public service management system that can be used for not just Aadhaar centers but also hospitals, banks, and many other government service providers.

REFERENCES

- [1] Unique Identification Authority of India (UIDAI), Aadhaar Authentication API Specification v2.5, Revision 1, Jan. 2022.

-
-
- [2] A. Soman, R. Patil, and S. Jadhav, "Mobile-augmented smart queue management system," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 2235–2241, 2020.
- [3] F. Ghazal, A. Kher, and M. Al Ahdal, "IoT-enabled smart queue management system," *Int. J. Comput. Appl.*, vol. 182, no. 48, pp. 25–32, 2015.
- [4] W. Tsai and C. Lin, "Applying multi-attribute value theory in patient admission management," *Healthcare Manag. J.*, vol. 9, no. 2, pp. 101–107, 2014.
- [5] A. Uzun, "QR-based arrival authentication in healthcare," *Int. J. Healthcare Informatics*, vol. 6, no. 3, pp. 55–61, 2016.
- [6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.
- [7] S. Murdoch, "Hybrid biometric identity management systems," *J. Secur. Privacy Digit. Identity*, vol. 12, no. 3, pp. 18–25, 2020.
- [8] M. Moreno, R. Neisse, and G. Baldini, "Blockchain-based decentralized identity management," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 2, pp. 140–147, 2021.
- [9] E. Ataelfadiel, "QR code and OTP-based two-factor authentication," *Int. J. Inf. Secur.*, vol. 15, no. 4, pp. 223–231, 2023.
- [10] D. Werner, H. Schmidt, and F. Müller, "Token-based identity management in cloud systems," *J. Cloud Comput. Adv.*, vol. 11, no. 5, pp. 325–330, 2017.
- [11] M. Awad, K. Singh, and P. Reddy, "AI-driven Aadhaar data analytics for governance," *Int. J. Mach. Learn. Appl.*, vol. 14, no. 1, pp. 55–64, 2024.
- [12] R. Ekansh, "Privacy-preserving Aadhaar authentication with blockchain," *J. Inf. Secur. Res.*, vol. 10, no. 2, pp. 42–48, 2024.
- [13] "Cross-platform Flutter-based mobile applications," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 6, pp. 120–126, 2022.
- [14] P. More, A. Patki, and R. Joshi, "Spring Boot framework for secure backend systems," *Int. J. Comput. Data Sci.*, vol. 5, no. 4, pp. 77–85, 2016.
- [15] A. Patki, R. Joshi, and P. More, "Smart queue management with real-time tracking using CNN and DNN," *Int. J. Recent Technol. Eng.*, vol. 8, no. 6, pp. 2235–2241, 2020.
- [16] N. Sharma and S. Rathi, "Context-aware queue management using IoT sensors in smart cities," *J. Emerg. Technol. Innov. Res.*, vol. 4, no. 5, pp. 325–330, 2017.
- [17] J. Mallari, M. S. Mallari, and K. B. Villanueva, "CLIQUE: A web-based queue monitoring system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 4, pp. 77–85, 2022.
-
-

-
-
- [18] R. Anand and D. Anand, “Aadhaar and India’s digital transformation: Opportunities and challenges,” *J. Inf. Secur. Appl.*, vol. 62, pp. 102–110, 2021.
 - [19] R. Deshmukh, H. Manvatkar, R. Malonde, R. Mahalle, R. Ramavat, and A. R. Bhuyar, “Smart card and QR-based Aadhaar authentication system,” *Int. J. Comput. Sci. Mobile Comput.*, vol. 8, no. 6, pp. 120–126, 2019.
 - [20] S. Mehta and K. Iyer, “QR code-based identity authentication for Aadhaar,” *Int. J. Secur. Privacy Digit. Syst.*, vol. 7, no. 2, pp. 101–107, 2019

VANRAKSHAK: AI-BASED WILDLIFE MONITORING SYSTEM USING ML MODELS

Professor. ¹Shravani Pawar, ²Sudhir Morchale and ³Prathamesh Shinde

¹Assistant Professor, Bharati Vidyapeeth's Institute Of Management And Information Technology Navi Mumbai, India

²Bharati Vidyapeeth's Institute Of Management And Information Technology Navi Mumbai, India

³Bharati Vidyapeeth's Institute Of Management And Information Technology Navi Mumbai, India

ABSTRACT

Monitoring wildlife is essential for the preservation of ecosystem balance, as well as preventing human-animal conflicts, especially in areas adjacent to forests. The growth of urban dwelling, deforestation and loss of habitat, have greatly increased the instance of human-animal encounters. Outdated methods such as camera traps, infrared sensors and manual patrols are generally costly, limited in coverage and do not provide real time alerts.

Vanrakshak has been developed as an intelligent monitoring system that utilizes a combination of machine learning and deep learning methods to detect animals in real time and send alerts when animals are detected. The detection of animals is accomplished via the Android application using YOLOv8; once an animal has been detected, a short video is recorded, and the GPS location is captured and uploaded to a cloud-based back end via Spring Boot and MySQL.

In addition, an admin dashboard is provided for logging detections, Google Maps integration, and the broadcasting of alerts to users in a timely manner. Vanrakshak offers real-time monitoring, an increase in user safety, and offers the ability to provide support for wildlife conservation efforts, via a scalable and cost effective solution.

Index Terms—Wildlife Monitoring, Machine Learning, Deep Learning, YOLOv8, Real-Time Detection, Android Application, GPS Tracking

I. INTRODUCTION

Monitoring wildlife is critically important in providing healthy ecosystems for both wildlife and humans and in protecting both wildlife and humans and from harm. Due to increasing human development practices and urban sprawl into previously undeveloped forest areas, more and more wildlife is moving into previously developed areas, thus having greater chances of encountering and damaging human infrastructure (buildings, fences, vehicles, etc.) and injuring themselves and/or humans. Wildlife encounter incidents such as those previously described require greater amounts of time, money, and other resources to deal with.

Traditional wildlife monitoring solutions rely heavily on manual patrolling, infrared cameras, and other sensor-based detection systems; these traditional wildlife monitoring solutions have substantial operational and financial limitations relative to their ability to respond in real-time to any type of wildlife encounter.

Heavy advancements in artificial intelligence (AI), machine learning, and deep learning now enable intelligent systems such as the Vanrakshak wildlife monitoring system to offer real-time detection, geolocation, and alerts through mobile devices and cloud-based infrastructure.

A. Background

Artificial Intelligence's (AI) integration with environmental monitoring systems is revolutionizing how people have tracked animals for years. Camera trap and manual observation have been limited because of their delayed response times and limited geographic area coverage. With the improvements in deep-learning and complex computer-aided detection of objects, wildlife can now be identified via image or video within milliseconds. The Vanrakshak employs these deep learning capabilities by using AI capabilities on portable, mobile-based devices.

Unlike traditional fixed-frame, stationary hardware systems, mobile devices provide greater flexibility to dynamically deploy monitoring equipment to forested areas. Greater flexibility means that authorities are more easily able to monitor wildlife in real time, while also reducing operational costs and improving the overall efficiency of monitoring by providing authorities with the ability to conduct continuous monitoring. Additionally, the increased integration of geographic tracking through GPS provides an additional level of intelligence about wildlife movements and a greater capacity for authorities to monitor, therefore improving authority's capability to provide animal movement data for further analyses to identify potential high-risk zones, to enhance the authorities' capability

to take preventive measures to make better decisions.

B. Motivation

- Increase in incidents involving conflict between people and animals
- No way to monitor wildlife in real-time
- High price of typical wildlife monitoring systems
- Need for solutions that can be easily scaled up and carried around.

C. Objectives

- 1) To create a system that detects wildlife in real-time; using YOLOv8
- 2) To have an Android application available for field use
- 3) To allow users to use GPS to tag the locations of animals they see
- 4) To set up a central database for storing information about animal sightings

-
-
- 5) To send notifications to users and agencies regarding wildlife sightings.

II. RELATED WORK

A. Wildlife Detection Systems

Wildlife detection systems employ Deep Learning Models like CNN, YOLO Faster RCNN. These models have proven to provide accurate results when identifying animals within both video images quickly.

B. AI-Based Monitoring Systems

Currently, various specific systems that combine Raspberry Pi computers with sensors; satellites; and drones provide a method of monitoring wildlife. Unfortunately, their ability to be integrated into cellular networks and/or to provide immediate notifications of wildlife activity is not currently available.

C. Research Gap

Most existing systems focus on detection but lack:

- Real-time alerts
- Mobile-based deployment
- GPS tracking
- Centralized cloud storage

III. PROBLEM DEFINITION

Wildlife monitoring faces several challenges:

- Lack of immediate detection/alerting systems.
- Dependence upon costly equipment.
- Limited range/scalability.
- Lack of geographic tracking and centralized data records.

IV. PROPOSED VANRAKSHAK SYSTEM

A. System Architecture

The system consists of:

- 1) Data Acquisition Layer (Camera Input)
- 2) Data Processing Layer (YOLOv8 Model)
- 3) Backend Layer (Spring Boot + MySQL)
- 4) Application Layer (Android + Dashboard)

B. Functional Modules

- Animal Detection Module
- Video Recording Module

- GPS Tracking Module
- Admin Dashboard
- Broadcast Alert System

Fig. 1. System Architecture of Vanrakshak

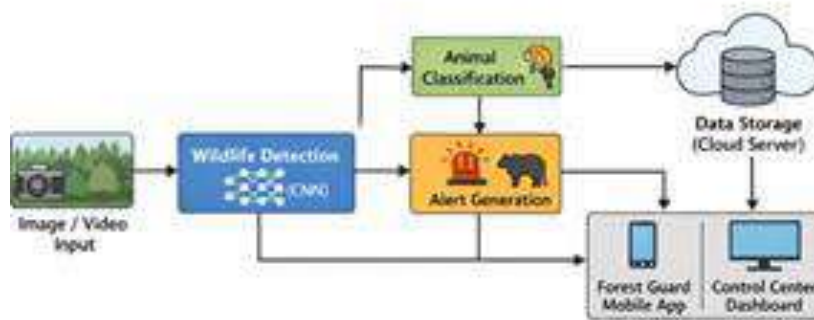


Fig. 1. System Architecture of Vanrakshak

C. Detailed Architecture Explanation

The layered architecture of the Vanrakshak system enables a continuous and efficient path for data to travel between the various layers of the system.

The Data Acquisition layer captures real-time video frames from a mobile device's camera. Once captured, the Data Acquisition layer sends the video frames to the Processing layer to allow the YOLOv8 model to complete an object detection on the video frame.

The Processing layer uses Convolutional Neural Networks (CNN) to extract the spatial features from the image (video frame) and identify objects in a predefined category (such as a deer, tiger, etc.). The Processing layer then completes the object detection process by executing other functions such as enabling the recording of the captured video and tagging of the location with a GPS marker.

The Back End layer provides a central destination for storing each of the detection log records from the Processing Layer, from captured video evidence to location data, as well as a central system for communication between the User and Administrator.

The Application layer provides a graphical user interface (GUI) for Users to use to access and view the alerts and real-time information available to them.

The layered architecture of the Vanrakshak system provides for scalability, modularity, and efficient processing of/open stream data.

V. DATASET DESCRIPTION

A. Wildlife Dataset

Includes images of animals such as tigers, elephants, deer, leopards, and boars.

B. Dataset Split

The dataset is divided into training, validation, and testing sets in an 80:20 ratio.

TABLE I DATASET STATISTICS

Dataset	Samples	Classes	Source
Wildlife Images	10,000	5	Kaggle
Custom Images	5,000	5	Field Data
Detection Logs	2,500	-	System Generated

VI. DATA PREPROCESSING

A. Image Preprocessing

- Image resizing
- Normalization
- Noise removal
- Data augmentation

B. Normalization Explanation

The normalization process plays a crucial role in improving the performance of the machine learning model. The equation used:

To avoid overfitting the model from across the training dataset, early stopping techniques have been applied which enables the model to generalize to new observations. This enables the model to have a high level of generalization when presented with previously unobserved data sets.

The validation dataset is used throughout the training process to monitor model performance and adjust parameters as needed to identify optimal parameters.

Batch processing methods and data augmentation (data augmentation refer to techniques for increasing accuracy of a model) have also been implemented to increase robustness, enabling the model to perform efficiently across a wide range of environments (e.g. different environmental lighting, angles and backgrounds).

IX. EVALUATION METRICS

I_{norm}

$I - \mu$

$= \frac{\quad}{\quad}$

σ

(1)

- Accuracy
- Precision

Where I represent input images, the input image's image values (pixels) are applied to the mean () and standard deviation ().

By performing this transformation, all pixel values are able to rescale into a more consistent range, which decreases

- Recall
- F1 Score

$$TP + TN$$

the influence of lighting variance and noise. Therefore, the model can concentrate on learning to identify patterns that are important instead of being adversely affected by variance in intensity. In addition, normalization decreases the time frame required for a model's AI data set's model to complete the training process and improves the convergence stability process.

VII. MACHINE LEARNING MODELS

A. YOLOv8 Model

The YOLOv8 model is used to identify objects in "real-time" within the category of wildlife species.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

$$TP + TN + FP + FN$$

Provides an overall measure of system accuracy. But for wildlife detection works will solely rely on the accuracy is not always enough for an effective measure.

- Precision provides a way in measuring the number of correct detections of animals.
- Recall provides a way in measuring the number of animals that have been successfully detected.

The F1 Score is a way of finding a balanced level between precision and recall measures and can be used as an overall evaluation metric.

$$P_i = \frac{\sum_{j=1}^n e^{z_j}}{n} \quad (2)$$

All of these measures provide realistic means of evaluating how well (II) works in the real world, but most importantly

VIII. TRAINING STRATEGY

- Loss Function: Cross Entropy
- Optimizer: Adam
- Early Stopping
- Validation

A. Training Optimization Details

The system training process for Vanrakshak has been optimally trained to achieve high levels of accuracy in detections while at the same time being able to perform in real-time. In order to optimize training convergence speed, the training uses an adaptive learning rate algorithm called Adam Optimizer as it has proven to improve training speed through its adaptive learning rate feature.

when missing a detection can cause safety-related issues

X. RESULTS AND ANALYSIS

TABLE II

PERFORMANCE OF VANRAKSHAK SYSTEM

Metric	Performance (%)	Accuracy
Precision	93	94
Recall	92	
F1 Score	92.5	

XI. CONFUSION MATRIX

Fig. 2. Animal Detection Confusion Matrix

		Predicted Class			
		Tiger	Elephant	Deer	No Animal
Actual Class	Tiger	TP	FN	FN	FN
	Elephant	FP	TP	FN	FN
	Deer	FP	FN	TP	FN
	No Animal	FP	FN	FN	TN

TP: True Positive

FN: False Negative

FP: False Positive

TN: True Negative

Fig. 2. Animal Detection Confusion Matrix

A. Confusion Matrix Analysis

The confusion matrix defined in Figure 2 displays how well the animal detection model performed by comparing actual class labels vs. predicted class labels in a table format. In the confusion matrix, each row of the matrix displays the actual class and each column of the matrix displays the predicted class. The diagonal elements of the matrix are the correct predictions of the model (i.e., True Positives (TP) and True Negatives (TN)). The off-diagonal elements of the matrix are the prediction errors made by the model. Off-diagonal prediction errors are classified as False Positives (FP) and False Negatives (FN).

A True Positive (TP) is when the model identifies as correctly as possible an animal as being part of the correct animal classification such as a tiger being identified as a tiger. A True Negative (TN) would be indicating that no animals have been identified correctly. A False Positive (FP) would indicate to the system that there has been an indication of an animal and that it therefore has no indication that an animal is present when in reality, it is not. This may generate unnecessary alerts. False negatives (FN) would be worst of all because they indicate that the system did not detect an actual animal; therefore, creating potential safety hazards for the user.

From the confusion matrix, one can see that classification errors are frequently made between visually similar classes, or in some cases due to environmental situations such as inadequate lighting or objects blocking the view of the model. Reducing the number of FP's is very important to this system as missed detections can create hazardous circumstances for the user.

Beyond the typical measure of accuracy of the model, confusion matrices provide additional details of how to increase detection performance and improve the overall detection capabilities of the model.

XII. DISCUSSION

The system demonstrates high accuracy and real-time performance. Integration with mobile and cloud improves usability and scalability.

XIII. ADDITIONAL FEATURES AND ENHANCEMENTS

A. Real-Time Alert Mechanism

The Vanrakshak has an alerting system that provides immediate notification from the detection module to the user once an animal has been detected. The detection module sends notifications to every user that has registered with the system, and they will receive detailed information about the location of the detection and any media evidence as well.

B. Scalability of the System

The system is architected to be highly scalable and deployable in many geographic regions with no adverse impact on system performance. The cloud based back end supports large numbers of users and detection events without degrading performance.

C. Security and Data Privacy

The system has methods for maintaining data security through secure API communications and reliable authentication methods. Any user's private and sensitive information (e.g., user data location data) will be tracked in such a way as to ensure user's privacy and security.

D. Practical Applications

The Vanrakshak detection system can be used in any number of practical ways beyond what was originally planned (e.g., wildlife management, vehicle safety while driving along high-ways, and wildlife conservation research). In addition to this, governments will have an easier time handling issues related to wildlife with these types of systems.

XIV. LIMITATIONS

- Low-light detection issues
- Internet dependency
- Limited dataset

XV. CONCLUSION AND FUTURE WORK

Vanrakshak provides a real-time wildlife monitoring system. Future improvements include night vision and offline mode.

REFERENCES

- [1] J. Redmon et al., "You Only Look Once: Unified Object Detection," CVPR, 2016.
- [2] Ultralytics, "YOLOv8 Documentation," 2023.
- [3] G. Jocher et al., "YOLOv8 by Ultralytics," GitHub Repository, 2023.
- [4] OpenCV Library Documentation.
- [5] Spring Boot Documentation.

AI OPTIONS TRADER – ADVANCED MULTI-TIMEFRAME ENSEMBLE SIGNAL ENGINE

¹Prof. Sudeshna Roy, ²Aniket Prakash Chougule and ³Suraj Jadhav

¹Master of Computer Application (MCA), Bharati Vidyapeeth's Institute of Management and Information Technology, CBD Belapur, Navi Mumbai

²Master of Computer Applications (MCA), Bharati Vidyapeeth's Institute of Management and Information Technology, CBD Belapur, Navi Mumbai

³Master of Computer Applications (MCA), ³Bharati Vidyapeeth's Institute of Management and Information Technology, CBD Belapur, Navi Mumbai

ABSTRACT

Cryptography trading is considered as one of the tough and little complicated field. It is open all the time, it does not have any central regulator. Therefore it is very different from other financial markets. because of that the prices of cryptocurrencies changes very quickly and cannot be predictable. Resulting doing trading in cryptocurrencies manually can be very challenging, and also does not work a lot.

Relative strength index and moving average convergence divergence this factors are mainly used in making traditional trading strategies. They are helpful but not that much good for dealing with such sudden changes in the market. They give signals but those may be confusing for traders.

Nowadays, Automated trading systems have become more popular with the help of Artificial intelligence and Machine learning. This systems find patterns also make predictions regarding future price movements after studying existing data. even so many of these systems acts like boxes resulting in very complicated for users to learn the process of make their predictions. As well they do not have strategies for risk management, which have impacts on practical use.

This research tells about a type of trading system which combines factors like machine learning models along with technical validation & management of risk. The objective is to create transparent system, adapting changing conditions of markets and also predicting prices.

Analysis techniques such as Relative strength index, Moving average convergence divergence and Exponential moving averages. Some more factors it uses like candlestick pattern recognition and fair value gap detection. Risk management which based on average true range helps user in adjusting stop-loss and take-profit regarding market volatility.

System having step-by-step process starts from collecting data preprocessing, training models then validating them and last generating signals. Results of Experiment tells that combining learning along with multi-timeframe confirmation resulting reduction in false signals & also helps in improving trading performance. The system has features like more consistent, reliable and having risk-reward advantage than that of traditional trading.

The cryptography market is fast growing also changed the style of people's trading. It is open for 24/7 means all the time available, also highly volatile and always active market. Therefore while trading traders cannot depends on human strategies because of price volatility. So, there is need of automated trading systems that can handles such complexity.

INTRODUCTION

Traditional trading approaches are based on indicators, like the Relative Strength Index, Moving Average Convergence Divergence and moving averages. While these tools are useful they have limitations when it comes to dealing with the cryptocurrency market. Cryptocurrency trading systems need to be able to adapt to the nature of the market. Cryptocurrency markets are constantly. Cryptocurrency trading systems need to be able to keep up with these changes. The cryptocurrency market is a field and cryptocurrency trading systems need to be able to handle this challenge. trading systems capable of handling such complexity.

Conventional trading methods mainly use indicators like the Relative Strength Index (RSI) Moving Average Convergence Divergence (MACD) and moving averages. These methods are used by trading systems that can handle complexity.

Conventional trading methods mainly use indicators like the Relative Strength Index (RSI) Moving Average Convergence Divergence (MACD) and moving averages. These indicators help us understand market trends and momentum. They usually work alone and only look at one timeframe. In volatile markets they can give wrong or mixed signals.

The use of Artificial intelligence and Machine learning in markets becoming very popular. Such technologies help us to analyze lot of real time data. They research patterns and relations so it is hard to see along with traditional methods. The ML models such as random forest & gradient boosting resulting very good at predicting outputs. Many of machine learning based trading systems having a lot of limitations.

Traditional trading strategies consistently use analysis indicators such as relative strength index. Moving average convergence divergence and Exponential moving averages are mostly used for finding trends and also entry exit points. Because of simplicity and ease of understanding makes these indicators more popular. They are not good for high volatile markets.

They depends on predefined rules and single time frame analysis. This reduces their ability to transform to changing market situations. Traders repeatedly get signals also delayed reactions & inconsistent outputs.

Integration of artificial intelligence and machine learning into trading systems is the only solution to overcome from these issues. This model can ability to process lot of data then find patterns and also make predictions. Algorithms such as random forest, gradient boosting and neural networks work better in predictions tasks.

Many of the systems are complex to learn. They act as black box models. This makes it difficult for users to trust on their decisions. This thing reduces confidence of user. Also making it complex to use such systems in real world trading.

Background

Since last ten years Algorithmic trading has changed a lot. Traditional trading systems used some rules including one is when to buy or sell at moving averages another is stock was oversold.

They helpless in unpredictable markets. Then machine learning came in. Helps systems to go beyond this simple rules. For analyze data, techniques such as decision trees, support vector machines and random forests were helped.

These methods helps to make predictions with more accuracy. But these methods comes with new problems like overfitting and it was very complicated to learn why they made such predictions. Then deep learning models such as long short-term memory networks progressed. It did an even good job at learning data overtime. These models need lot of data also powerful computers and along with that it's still difficult to understand how they make their forecasts. Coming with all these advantage lot of trading systems still how predicting & checking and managing risk as diff things. This way does not work good because its all dividing.

So people need a system that mix-up making predictions with checking & controlling risks. Another big challenge in forecasting markets is that its all uncorrected and unpredictable. How people feel about the market how much money is available & how much quantity is being traded and unexpected events are some things directly impacts on momentum of prices.

Some old statistical models fight with all these relationships, which limits how good the can forecast. Machine learning though is better at looking patterns and connections in variables, which making it better, for analyzing existing financial data. Where patterns are not always in flow.

In spite of their advantages machine learning models wants designed features to work good. Raw market data is not that well to get insights. Therefore feature engineering might be important in process of turning data into useful information that makes models work well. The technical indicators which made from price and volume data give insights by studying volatility, momentum and trends.

Machine learning models have ability to learn market behavior even better when we add price action things such as candlestick patterns and structure of market. This things helps model to learn market behavior even good than human does. Two keys to getting insights from market are machine learning models & feature engineering.

For making machine learning model, feature engineering and technical indicators are really important factors. Making sure the signals are good enough is another important thing. When getting signals for short time periods they can be incorrect because of scenarios happening for time.

This results in make the outputs not reliable. On other hand stalking at longer time periods gives you good view of what exactly happening right now in the market but it can be difficult to find a good entry point of market.

Use of time periods helping a lot to traders because they able to view both big picture and small details. This path gave opportunity for match up long term trends with short term chances. People think that this is a path of making trading accurate but it is not actually used in automated systems.

Moreover trying to forecast what exactly happen and making assurance about signals are better a trading system also needs to have ability to manage expected risk. Even the better forecasting models can make mistakes. If you are not able to manage risk you can lose a lot of your money in few trades. Rather than using fixed plan it is better way to do things in live markets, making strategies is one of the best risk management theory. For making a good trading system feature engineering, technical indicators with validation as well as risk management are very much important.

OBJECTIVES

The first and main goal of research is to build a trading system. Using machine learning techniques to make sure the signals of trading are reliable and also a consistent towards time intervals. Meaning of this is we shall look at trends of market on various time frames. Examples like 1 hr., 15 min, 5 min charts.

Indicators such as RSI, EMA and MACD are good sense of markets trends that we want to use. In addition to that we go through the price action patterns, like candlestick for learn about market better. Trading system shall using Average true range for risk management. Meaning that system will adjusting stop loss and also take profit levels depends on volatility of market.

One more goal is to reduction in trading signals. We will achieve this by using validation layers, that includes machine learning predictions & technical confirmations. This helps the system make more correct predictions and also improving entire performance. For understanding how the system works the trading system keep logs of trading decisions.

This research targeted to making trading system reliable and more transparent. We want users can trust our system and learn the reason behind its given decisions. Using combine factors like indicators & machine learning techniques system providing clear directions into operations. This helping a lot to users for making trading decisions also improving entire performance of system.

Creation of system that is dynamic and also adaptable is our main focus. After responding changing market situations with adjustment of its risk management art as needed. This leading to help protect capital and also maintain a risk reward proportion. Entire the goal of research is to build trading system that is more correct, transparent and also reliable.

To get assurance of trading decisions are enough consistent across various time frames the trading system shall use timeframe validation. This way will help figure out noise and reduction in similarities of signals. System will be able to create informed decisions after analyzing markets trends on various time bounds.

To improve quality of forecasting we have option to use a set of technical indicators. These helps to catch momentum and also trend direction giving insights in market situation. After combining these indicators along with price action techniques for generation of signals that are enough accurate and reliable.

Main motive behind research is to improve trading system efficiency. The system will enhance performance and consistency in trading by reducing signals of trading and improvement of signal quality. The final milestone is to build trading system that is more reliable, transparent & accurate that gives users with information they needed to create good trading decisions.

LITERATURE REVIEW

In last few years the use of machine learning in markets has been studied a lot. It is very true when we trying to find out prices movements and when to buy or sell. At very first people used methods such as linear regression, decision tree and support vector machine. These ML methods were better at figure out patterns in price data structure. It did a good job of forecasting prices than that of traditional methods.

In many cases they were not good at facing with changes in market and also prices that was not follow a line, which is more common when you trades in cryptography.

People starts with use methods which is combined of ML models such as random forests & gradient boosting. Helping to make predictions accurate and more reliable. These ML models works by combine effects of results of models, results in reduction of chance of getting it incorrect and also makes create predictions more common. Because of having ability to handling noisy data and complex relations between various items these ML models are better at forecasting prices in markets and this shown in research.

Along with this advantages many of trading systems which uses machine learning are still have not enough transparency which making it difficult for peoples to learn how they build predictions and also trust them while making trades.

Machine learning is not only the path to make trade decisions but also look over the charts and trends. To find trends means see how fast prices were moving and find out when prices may be change direction peoples use things such as RSI, moving averages and MACD. Complex methods such as stalking candlestick patterns and also price movements can give little more insight into what actually market doing now.

Depending on these kind of methods may lead to inconsistent results because they might be give false of little conflicting signals and that factor can lead confusion for

people who trying to build trading decisions depending upon ML and technical analysis of many financial markets and also cryptocurrency trading.

Depending upon these advantages many systems which use ML are still not clear which makes it difficult for people to learn how they create predictions and also trusting on them when doing trades.

People who depending on methods to create decisions can getting incorrect results. This is only because of these methods consistently give signals. It can be getting confusing for people who trying to create decisions based on ML and cryptocurrency trading. Especially it is very complicated when market is over to the place.

Systems required a lot of data and little powerful computers. Also it is difficult to learn how they create decisions, which makes them little less suitable for trading. In trading it is really important to understand how decisions are made.

Another important thing is managing risk. Many trading systems use fixed stop-loss and take-profit levels. These levels do not change when the market changes. Studies have shown that using volatility based risk management techniques is important. These techniques use the Average True Range to adjust trading parameters.

These approaches have been shown to make trades last longer and reduce losses.. Combining dynamic risk management strategies with machine learning based prediction systems is still not common.

PROBLEM STATEMENT

Cryptocurrency trading is very tough. This is because it is highly volatile and happens all the time. There are also price swings. Traditional trading approaches use indicators like RSI, MACD and moving averages. These indicators give buy and sell signals.. These indicators often work alone. They are not good at adapting to market changes. As a result they often give signals. This is especially true in market conditions. It leads to trading decisions and financial losses.

With more people using machine learning in markets predictive models have been introduced to improve trading accuracy by looking at old data and finding complex patterns. While these models are better than methods they also introduce new challenges. Many machine learning models are being used in cryptocurrency trading and markets. Cryptocurrency trading and markets are using machine learning to make predictions. Machine learning and technical analysis of markets and cryptocurrency trading are being used together to make trading decisions. The market and cryptocurrency trading are very important, to people who are using machine learning and technical analysis to make decisions.

Systems work like a box that you cannot see inside they make predictions. Do not explain how they got those predictions, which makes users not trust them very much and they are not very useful in real life. Also these systems are usually trained with data and they have a hard time adjusting to changes in the market that happen very quickly which makes them not work well when things are happening in real time.

Another big problem with systems that exist now is that they do not handle risk well. A lot of systems use strategies to decide when to stop a trade or take a profit but these strategies do not take into account how much the market is changing. In markets like the one for cryptocurrency which's very unpredictable using these simple strategies can cause trades to end too soon or result in big losses. Because systems do not have a way to check if their signals are correct the signals they produce are not very reliable.

In addition to these problems systems that use machine learning and traditional methods of analyzing the market are not usually connected. Each method has its strengths but they are often used separately which means they do not work as well as they could. There needs to be a system that combines machine learning, technical analysis and risk management into one framework. This system should not make better predictions but also provide results that make sense and work well in different market conditions.

Machine learning methods have been used to try to fix some of these problems by allowing systems to find patterns in data and make predictions based on that data. Trading systems like these can learn from cryptocurrency markets and other markets and trading systems can make data-driven predictions, which's a big improvement over systems that do not use machine learning.

Using these approaches having made predictions very accurate. In many cases they also have some issues. Many ML models were such as boxes. they do not have ability to explain how they create predictions. This making it difficult for many users to trust them.

It is also complex to check if the signals which they are giving are reliable. Machine learning models can also have sensitive modifications in market. They may not able to work with data. One more big problem with systems is that they do not having any validation methods. Signals getting from one timeframe may not able to show entire market trend.

They may be affected by a short term volatility. These signals can lead to very bad decisions without checking timeframes. Many of systems do not combine the study with machine learning forecasting. This can leads to limits their abilities to use both things domain knowledge and date insights. finally results in they failed to develop trading strategy.

Management of risk is also one of concern. Many of solutions come up with the use of stop loss and take profit strategies. These can not be adapting changing market conditions. These can lead to early exits or big losses. The lacking in risk control gets making trading system less effective. It increases chance of outputs.

The system must give clear explanations and provide predictions. Traders always need a signals. Without giving any explanation is it difficult to trust on automated trading system. This clearly shows need of a system which balances accuracy as well as transparency.

It must be good working in market situations. Therefore main problem is that this research is addresses is a creating system which is integrated as well as smart & explainable. It providing signals by combining various methods. After every prediction there must be explanations. It also has ability to adapt market situations. Traders have to trust on signals it gives. System improves trading results with helping a lot to them.

METHODOLOGY

The system proposed is very simple and using machine learning and technical analysis for generation of trading signals for who going to trade. it starts by fetching real time market data from the official cryptocurrency exchange API. That data including very high low closing prices with trading volume. After that this raw data is going to cleaning up which meaning is handling missing values and removing incorrectness and then transforming data into a format which is easier to analyze. The system looking for information which can help improve the model once the data is clean. Strength index and moving average convergence divergence this kind of indicators system uses. Also it uses stuffs such as candlestick recognition & fair value gap detection for capture prices action behavior.

After that data is labeled into three parts which are buy, sell & hold based on price actions. For forecasting what things will happen system uses this ML techniques. It trains models such as random forest and gradient boosting on data. After combining their outcomes. This going to help to reduce overfitting and also making system accurate. System checks predictions across time intervals such as 1 hr., 15 min, 5 min. This gives assurance that trading signals were consistent and reduced impact of noise. The system also has feature of risk management mechanism depending upon average true range. It adjusting stop loss and take profit levels regarding to market volatility, which is trading signal system. For proposed system the trading signal system is really important. It uses it to make predictions.

SYSTEM ARCHITECTURE

Trading signal system is about how it uses machine learning for generating trading signals for system. The system helps trade adjusting to change conditions and improving risk control. This also helps to keep record of all decisions it makes.

It is really helping for making it easier to check how good trading signal system working. The system is combination of machine learning, risk management and technical analysis. This makes it good and easy for trading. Multiple timeframe helping to analyze both short term and long term market trends. The data which is collected is consistently updated at regular time intervals, and enables system to operate in real time situations.

Next layer consisting data preprocessing and also feature engineering section, in which raw data going to transform into well-structured format comfortable for machine learning.

This stage also including cleaning dataset by handling the missing values also removing incorrectness and standardizing data. Above preprocessing and feature extraction is important.

It brings together data processing, machine learning, validation and risk management into one workflow. The architecture starts with a data collection part. This part gathers time and historical market data from a cryptocurrency exchange API. The data includes opening, high, low and closing prices, trading volume and timestamps. This data is the base for analysis. The collected data goes to a preprocessing part.

Here it is cleaned, normalized and changed into information using indicators like RSI, MACD, EMA and ATR. Other analysis tools, such, as recognizing candlestick patterns and detecting Fair Value Gaps (FVG) are also used to make the data more valuable. The AI-based trading system uses machine learning models.

These models are a combination of models. The AI-based trading system uses these models to make trading decisions. The machine learning module uses the processed data. This data helps the AI based trading system to learn and make predictions. The AI-based trading system relies on machine learning. Machine learning helps the system to make trading decisions.

The data is then sent to the machine learning part of the system. This is the core of the system. It uses a method called learning. This means it uses models like Random Forest and Gradient Boosting. Each model looks at the data.

To get assurance the predictions are well system checks them a times. It looks over the predictions, in time frames like 1 hr., 15 min & 5 min. This thing helps to get rid of forecasting not strong. It making system more reliable also helping make well trading decisions.

The also having part to manages expected risk. This is also very important to protecting your money being used & making sure trading goes in good manner. The fixed rules were used for as average true value to decide stop loss and take profit decisions. This shows how volatile market is.

RESULT ANALYSIS

Performance of given ai based trading system was checked by using classification metrics and also trading specific indicators for accessing effective in real world situations. The ensemble model which is combination of random forest and gradient boosting with a voting process showing improved capacity compared to those models.

Metrics used for this is accuracy, recall, and f1 score for measuring the classification performance of AI based trading system. The result is balanced and consistent predictions by reduction of bias and variance.

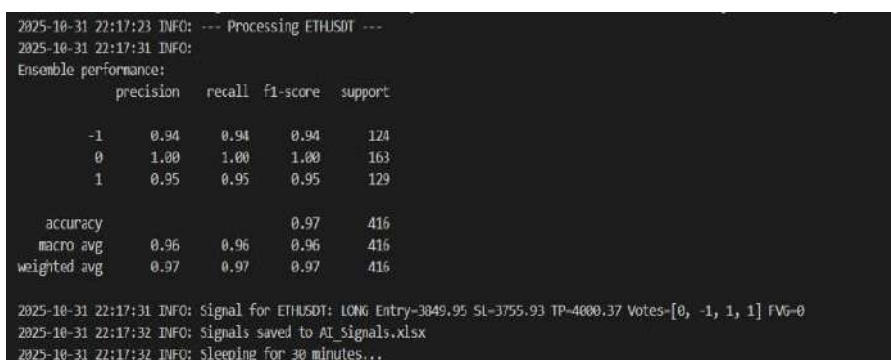
The main observation from analysis was an impact of multi timeframe validation at signal reliable. After studying all time frames resulting in making a strong signal for buy or sell. Also reduction in weak signals. And it is more effective in validation strategy.

The indicators contributed positively to ai based trading system performance. Indicators like RSI, EMA and MACD helped to fetch market trends and momentum. Combination of both candlestick patterns & fair value gap enhanced both the accuracy and of reliability of generated signals for decision making.

Risk management strategy played a role in achievement of results depending on average true range. Upon adjustment of stop loss and take profit levels based on market volatility then ai based system helps to protect capital of people. This changing approach gets assurance of trades were aligning to preventing market conditions which results in stable & consistent performance over a time.

In addition the logging and more tracking mechanism giving insights into the behavior of this system. Enabling a back testing and performance analysis done by recording generated signals and included executed trades.

The highlighted areas were analyzed where ai based system could further checked like incorporating features. Entire results applies that this system offers an improved version than that of traditional system. Combination of muti time frame validation, learning and technical analysis results in reliable and also efficient framework. The all results suggest that an integrated way is best for handling difficulties of cryptocurrency markets and also has more potential for real world application.





CONCLUSION

The entire study presenting ai based trading system. It being used machine learning, risk management and technical analysis for making trading decisions. The system is being trying for fixing problems all trading systems. It making predictions which is more accurate.

It going to works well in changing cryptography market. Random forest and gradient boosting this two models used in system. This models works together for making predictions. It also checking data from timeframes for figure out bad signals. For that it uses indicators to learn market situations.

System manages risk well. It adjusting stop loss and take profit levels depending on market fluctuations. Making trade more reliable and clear. It also improving trading performance and handling real life conditions. All this works good in financial markets.

REFERENCES

1. J. Patel, S. Shah, P. Thakkar, and K. Kotecha, "Predicting stock price index movement using Trend of present. Deterministic of Data Preparation and machine learning of techniques," Expert Systems with a great Applications, vol. 42, no. 1, pp. 259–268, 2015.

-
-
2. S. M. Idrees, M. Alam, and P. Agarwal, "A prediction path for stock market volatility depending on time series data," IEEE International Conference on Computing, Communication & the Automation, pp. 799–804, 2019.
 3. A. Ariyo, A. Adewumi, and C. Ayo, "Stock price prediction by using the ARIMA model," UKSim-AMSS Zu 16th International Conference on Computer Modelling and Simulation, pp. 106–112, 2014.
 4. S. Hochreiter And J. Schmidhuber, "Long short term memory management," Neural Computation, volume. 9, no. 8, pp. 1735 1780, 1997.
 5. T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery with Data Mining, pp. 785–794, 2016.

A COMPARATIVE STUDY OF MACHINE LEARNING MODELS FOR CHILDHOOD OBESITY RISK PREDICTION USING ANTHROPOMETRIC, LIFESTYLE, AND SOCIOECONOMIC DATA

¹Dr Nidhi Poonia, ²Gayatri Mahajan, ³Aarti Pansare and ⁴Tanishq Praveen Chand

¹Assistant Professor, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

^{2,3,4}Student, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

ABSTRACT

Due to rapid lifestyle changes, unhealthy eating habits, and lower levels of physical exercise among kids and teenagers, childhood obesity has become a serious public health concern. To prevent long-term health consequences, such as diabetes, cardiovascular diseases, and metabolic disorders, it is critical to identify obesity risk as soon as possible. In order to predict childhood obesity levels by analysing anthropometric, lifestyle, and demographic characteristics, this study compares several machine learning algorithms. Age, height, weight, frequency of physical activity, food habits, screen time, and sleep length are all included in the dataset. Performance indicators, including accuracy, precision, recall, and F1-score, are used to evaluate machine learning algorithms, such as Decision Tree, Random Forest, and XGBoost. According to empirical results, ensemble models XGBoost and Random Forest in particular achieve higher prediction accuracy than the Decision Tree model. A Streamlit-based interactive dashboard that makes it easier to visualise obesity trends and do real-time predictive analysis is added to the suggested architecture. The performance of machine. Early evaluation of the decision support systems is powered by learning. of the risk of obesity and the employment of an obesity preventive healthcare. This study supports the use of strategies.

I. INTRODUCTION

The frequency has increased considerably over the past. Childhood obesity has evolved to be a huge worldwide issue over the decades. World Health Organisation documents that shift in food preferences, urbanization, and lifestyle have caused. To a considerable rise in the level of overweight and obese children [10]. There is co-existence of inadequate nutrition and excess weight. in developing nations such as India, the establishment of complex health is formed. problems that must be efficiently tracked down and addressed in time. [11]. A number of researches have been conducted on machine learning. predictive methods of pediatric obesity using lifestyle and healthcare data. Deep learning models applied to. Identify the risk of obesity with electronic health record data. Gupta et al. proved better predictive efficacy. [1]. On the same note, Pang et al. [2] used large clinical datasets. Random Forest and Logistic are machine learning techniques for the prediction of early childhood obesity regression.

Furthermore, the increasing importance has been noted by studies based on surveys of machine learning on health management analytics, particularly in predicting risk factors of obesity and enhancing decision support systems [3]. The recent studies have been centred on the determination of major. lifestyle and behavioural causes of obesity. The findings of empirical studies show that physical, but not sedentary, behaviours, are related to them. A strong impact has been seen on the activity levels and dietary habits on obesity outcomes [6], [7]. Moreover, ensemble learning comparison model evaluations and techniques have been utilised to achieve more prediction reliability and accuracy [5], [8]. Additionally, educative predictions are being reported. tors and medical workers making use of interactive dashboards. and visualisation tools, which enhance the understanding and preventive health maintenance planning [9]. These developments illustrate the ways machine learning-based systems could be used to assist in the intervention and diagnosis of Obesity in minors.

A. Motivation

The following crucial findings from recent research serve as the foundation for the suggested Childhood Obesity Prediction System:

- The concerning rise in childhood obesity due to changes in Life practices, poor eating habits, and more sedentary activities [6]. Conventional approaches to measuring obesity, which primarily rely on Body Mass Index (BMI), sometimes fail to consider the influence of environmental and behavioural factors [3].
- The need for early predictive models that use machine learning techniques to simultaneously assess several factors [5]. The lack of data-driven wellness care decision- support tools that help Medical care professionals and educators identify risk factors for obesity [9]. The integration of machine learning with Clinical care data to improve preventative Patient care programs is gaining scholarly attention [8].

B. Objectives

The principal aims of the proposed Childhood Obesity Prediction System are as follows:

- 1) To construct a machine learning-oriented system proficient in forecasting childhood obesity levels by utilising Somatic measurements, Standard of living, and Habitual datasets.
- 2) To execute a comparative analysis of supervised machine learning algorithms, including Decision Tree and Random Forest, for multi-class obesity classification.
- 3) To ascertain the critical determinants that contribute to obesity risk through the application of feature importance analysis.
- 4) To examine Living style and Habit-based patterns correlated with childhood obesity employing data-driven methodologies.
- 5) To devise an interactive dashboard that effectively visualises overweight trends

and facilitates early risk assessment for preventative healthcare measures.

II. RELATED WORK

In order to address the growing prevalence of obesity in pediatric populations, several studies have investigated juvenile Excess body weight prediction using machine learning and health informatics techniques.

A. Predicting Childhood Obesity Through Machine Learning

Using electronic health record datasets, Gupta et al. [1] used deep learning architectures to predict obesity susceptibility while maintaining results interpretability. The effectiveness of machine learning methods, such as Random Forest and Logistic Regression, in the early prediction of childhood obesity was demonstrated by Pang et al. [2]. Additionally, survey-based research has highlighted the growing importance of machine learning techniques in the field of healthcare analytics [3]. Additionally, it was shown by Patel and Singh

[5] and Mondal et al. [4] that both supervised and ensemble learning approaches can effectively classify body weight risk.

B. Behavioral and Lifestyle Factor Analysis

The risk of obesity is significantly influenced by lifestyle and behavioural factors, according to Applied research. Ahmed and Hussain [6] and Sharma and Verma [7] emphasised how important sedentary lifestyles, dietary habits, and physical

activity are to Excess fat accumulation prediction models. To identify important risk variables from complex datasets, ensemble learning and feature selection techniques have also been used [8].

C. Decision-Support Systems and Visualization

In order to improve interpretability and accessibility, recent research has combined machine learning models with visualisation tools. While worldwide evaluations from the World Health Organisation [10] and studies on obesity trends in India

[11] Highlighting the need of early detection, Sharma and Mahajan [9] developed interactive healthcare dashboards focused on predictive analytics. These decision-support systems could help educators and healthcare professionals identify children who are at danger and carry out prompt treatments [12].

III. PROBLEM STATEMENT

Due to children's decreased physical activity, poor eating habits, and increasingly Idle lifestyles, childhood Adiposity has emerged as a significant global public health concern. Global health reports state that over the past few decades, childhood obesity has become much more common, which has resulted in major long term health issues[10], [11]. Therefore, it is crucial to identify obesity risk early in order to promote preventive healthcare initiatives.

Traditional obesity assessment methods mainly rely on body mass index (BMI) and basic Body size metrics.

However, these measures alone do not capture important lifestyle and behavioural factors such as dietary habits, physical activity levels, and screen time, which play a significant role in obesity development [6], [7].

Several studies have used machine learning techniques to analyse healthcare data and improve the Validity of obesity prediction [1], [2]. However, many existing approaches focus mostly on clinical data and often ignore behavioural and environmental factors.

Also, numerous machine learning models designed to be used in Weight status predictors are not interpretable and hard to comprehend in practical applications like schools or communities. Healthcare systems and healthcare practitioners, and educators require readable knowledge in order to establish significant risk variables and act in advance, although predictive models are able to do so attain high accuracy and childhood can be successfully forecasted, prevent early preventive action and assist in risk and obesity. Explainable machine learning-based system with incorporation, One needs anthropometric, lifestyle and demographic information [8], [12].

IV. PROPOSED PREDICTION SYSTEM FOR CHILDHOOD OBESITY

A. System Architecture

The proposed model of childhood obesity prediction. is scalable and modular, merging the aspects of data processing, machine learning, and visualisation. The following layers constitute the overall architecture:

- 1) Data Acquisition Layer** - demographic, lifestyle, and anthropometric measurements on obesity among children. Preprocessing and Exploratory Analysis Layer Data.
- 2) Scales features-** Encodes categorical variables. data cleaning, missing value management. Finding patterns and associations among variables, exploratory data analysis through visualisation is conducted with the use of visual- ization tools.
- 3) Machine Learning Layer** - Foretells the level of obedience. trained on the processed data with the help of supervision. Random Forest and Decision Trees are some of the learning techniques. Tree.
- 4) Application and User Interface Layer** - Presents. results through an interactive dashboard developed using Streamlit, which allows users to view trends and estimate their likelihood of obesity.

B. Functional Modules

The following functional modules make up the proposed system:

- 1) Data Preprocessing Module** – This module processes. fills in missing values, added features and universalises numerical attributes.

-
-
- 2) **Exploratory Data Analysis Module** – This is a module. relies on visualisation software such as Power BI to study data. relationships among the levels of obesity and lifestyle predispositions.
 - 3) **Machine Learning Model Training Module** uses the prepared dataset to train predictive models, such as Decision Tree and Random Forest.
 - 4) **Obesity Prediction Module** predicts the obesity levels of Models used to generate new input data.
 - 5) **Model Evaluation Module** estimates the performance of models. applying such measures as accuracy, precision, recall, F1-score, and confusion matrices.
 - 6) **Feature Importance Module**: The module is based on features. importance analysis to determine important factors increasing the risk of obesity.
 - 7) **Streamlit Interactive Dashboard Module** - Facilitates parameters that are entered by users into the system to predict real-time obesity. and visualises trends of obesity.

V. WORKING

The initial phase of the proposed Childhood Obesity Prediction system will be the collection of structured data sets that include. demographic, behavioural, and anthropometrical features. linked to obesity risk. To ensure data consistency and boost model execution, the dataset is preprocessed by handling missing data, processing the categorical variables, and performing feature scaling. In the following, there would be patterns and relationships among lifestyles. Exploratory data is used in determining choices and obesity levels. analysis, or EDA. Such revelations help in the understanding of the. The effect of such variables as physical activity, diet, and demographics on the results of obesity. The supervised training is done using the transformed dataset. Random Forest and Decision Tree machine learning algorithms. Tree. Measures of performance such as accuracy, precision, and recall. The performance of the model is evaluated using F1-score and confusion matrices. The models acquire correlations among input variables and obesity categories. Finally, the trained model will be integrated with an interactive. Streamlit-based dashboard to allow users to input personal. traits, refer to obesity trends, and receive real-time obesity. level forecasts. This is a more effective methodology for measuring the risk of early childhood obesity and preventive medical decisions. through the provision of a clear and easy-to-use solution.

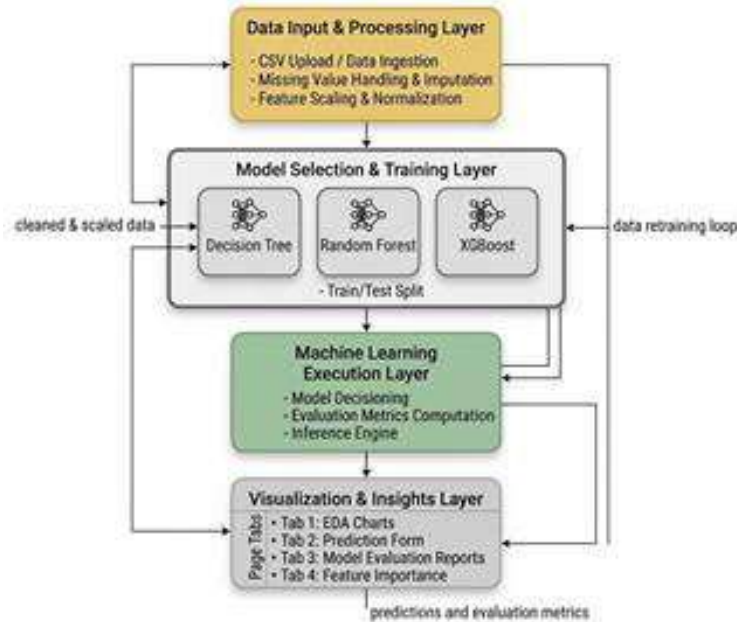


Fig. 1: System Architecture Diagram

The workflow of the proposed Childhood Obesity Prediction system includes data entry and pre-processing, and machine learning. Model training and evaluation is represented by the system. architecture diagram. Proper prediction of the level of obesity and The visuals and insights allow performing risk analysis. shown in the final layer.

VI. DATASET DESCRIPTION

A. Anthropometric Dataset

Measures like age, height, weight, and Body Mass Index (BMI), which are often used indicators for determining obesity levels, are included in this dataset.

B. Lifestyle Dataset

Physical exercise frequency, vegetable and water intake, screen time, sleep duration, and technology usage habits are among the behavioural characteristics included in the lifestyle dataset.

C. Demographic Dataset

Gender, family history of obesity, and method of transportation are among the demographic details included in this dataset.

D. Split Dataset

To assess the effectiveness of machine learning models, the dataset is split into training and testing sets at a 70:30 ratio.

TABLE I: Dataset Statistics		
Dataset Type	Samples	Classes
Obesity Dataset	2,111	5

VII. DATA PREPROCESSING

A. Data Cleaning

- Handling missing values
- Removing inconsistent or contradictory records

B. Feature Engineering

- Label encoding of categorical variables
- Feature scaling and normalisation

VIII. MACHINE LEARNING MODELS

A. Classification Models

The following supervised learning algorithms are used to predict obesity:

- Decision Tree
- Random Forest
- XGBoost

B. Baseline Model

- Logistic Regression

IX. TRAINING STRATEGY

The models are trained using a supervised learning approach with the following strategy:

- Loss Function: Categorical Cross-Entropy
- Train–test split validation
- Performance metrics: Accuracy, Precision, Recall, and F1-score
- Confusion matrix analysis

X. END-TO-END WORKFLOW DIAGRAM

The end-to-end workflow diagram shows the entire Childhood Obesity Prediction system process. Gathering and preparing the dataset, which includes feature scaling, encoding, and data cleaning, is the first stage in the pipeline. The processed data is then used to train machine learning models such as Decision Tree, Random Forest, and XGBoost. After the model is evaluated using performance indicators, the results are presented using an interactive dashboard that enables the prediction of obesity risk and the presentation of significant insights.

Diagram:End-to-End Workflow Diagram

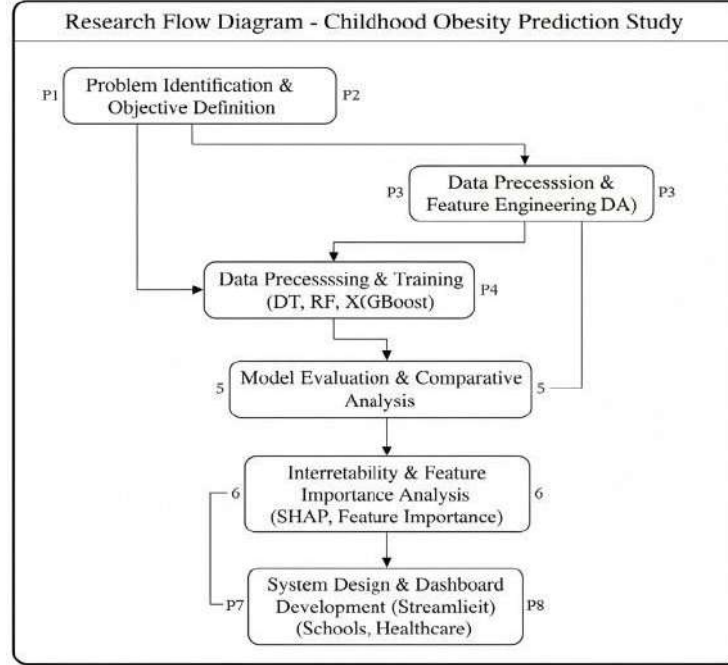


Fig. 2: End-to-End Workflow

The general procedure of the Childhood Obesity Prediction study is presented in the research flow diagram, i.e., the identification of the problem and the preprocessing of the data are followed by the training of the machine learning model. The next steps in the workflow include the evaluation of the model, analysis of features, and the development of a dashboard based on Streamlit that can be used to visualise and make predictions.

XI. EVALUATION METRICS

The following metrics are used to assess the effectiveness of the suggested Childhood Obesity Prediction system:

- Accuracy
- Precision
- Recall
- The F1-Score
- ROC-AUC

TABLE II: Accuracy and Weighted Performance Metrics of Machine Learning Models

Fig. 1. Metric	Fig. 2. Decision Tree	Fig. 3. Random Forest	Fig. 4. X GBoost
Fig. 5. Accuracy	Fig. 6. 93.8534	Fig. 7. 94.7991	Fig. 8. 96

			.2175
Fig. 9. Weighted Precision	Fig. 10. 93.9536	Fig. 11. 94.7698	Fig. 12. 96.2649
Fig. 13. Weighted Recall	Fig. 14. 93.8534	Fig. 15. 94.7991	Fig. 16. 96.2175
Fig. 17. Weighted F1-Score	Fig. 18. 93.8265	Fig. 19. 94.7651	Fig. 20. 96.1989

The weighted evaluation criteria and the accuracy of the machine learning models applied to predict childhood obesity. Random Forest and XGBoost were doing better in all metrics. But the Decision Tree did not do so well as the other models.

XII. MATRIX OF CONFUSION

The confusion matrices indicate the correct predictions, and the classification is analysed using patterns of misclassification. results of Decision Tree, Random Forest, and XGBoost. models across various categories of obesity.

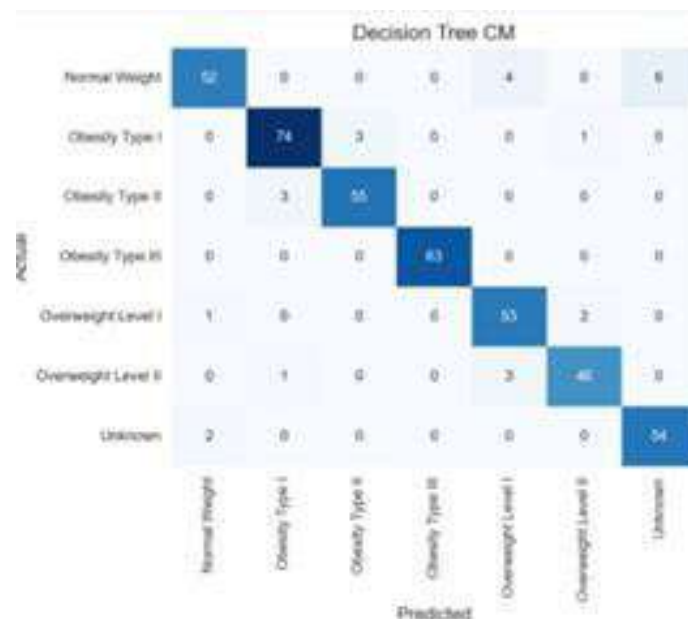


Fig. 3: Decision Tree Model Confusion Matrix

The misclassifications between the neighbouring levels of obesity are noticeable, though the Decision Tree confusion matrix decreases. classification performance, which implies poor generalisation in dealing with complex classes.

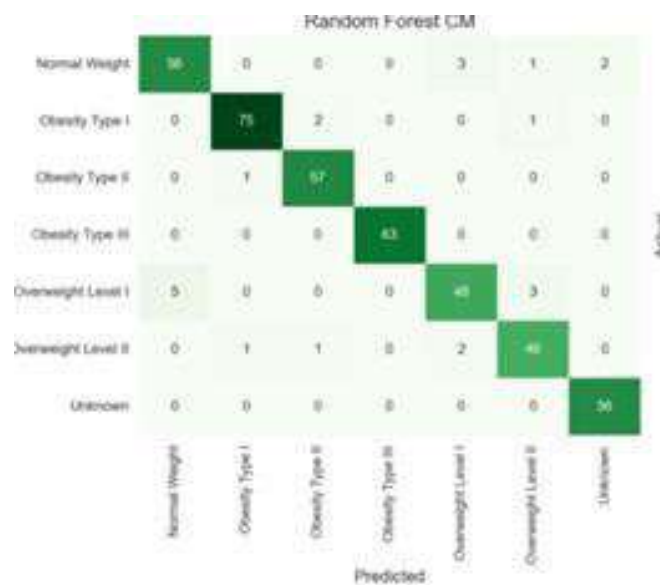


Fig. 4: Confusion Matrix of Random Forest Model

Comparing it to the Decision Tree model, the Random Forest confusion matrix has better diagonal dominance, which points to a higher number of class-wise correctness and a reduction in misclassifications.

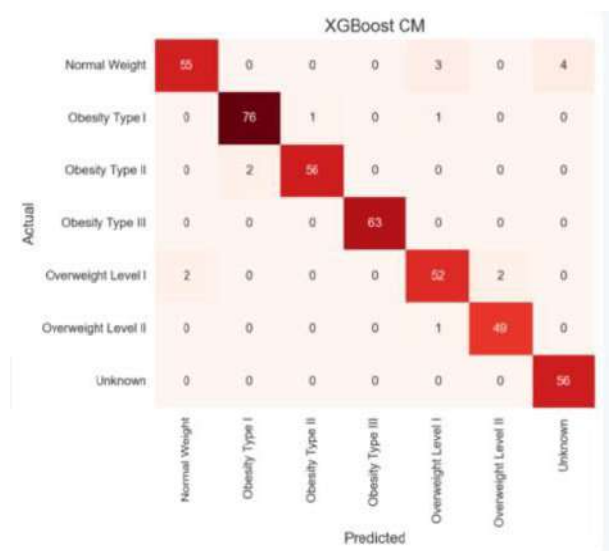


Fig. 5: Confusion Matrix of XGBoost Model

The XGBoost confusion matrix proves its effectiveness in (not) controlling complex interacting features through the exemplification of good. Poor errors in prediction across the category of obesity.

XIII. DISCUSSION

The results of our experiment confirm that the proposed Childhood Obesity Prediction system, combining anthropometric, lifestyle, and demographic data with the help of machine learning, is valid. The framework effectively performs better than existing methods. Ensemble models, such as those in the comparison research, suggest that the models used are ones where multiple models are combined into one to yield the desired result (Cambridge Dictionary, 2019). Random Forest and XGBoost achieve higher class-wise performance and prediction accuracy than single models, such as Decision Tree.

Based on the efficient models, it was possible to enhance model resilience and minimise noise caused by inconsistent and incomplete data. characteristics, engineering and data preparation. Beyond conventional Assessments based on BMI, the inclusion of lifestyle factors, including physical activity, food preferences, screen time, and sleep patterns, highly enhanced prediction accuracy. Scalability, interpretability and intuitive interaction are. enabled by the modular design and Streamlit-based interface of the system. The strategy is especially effective in the Indian setting. is quite applicable to practice in such an environment as in schools.

XIV. RESTRICTIONS

The following are the constraints of the suggested system:

- Self-reported lifestyle data must be accurate and comprehensive.
- In comparison to large national or international health datasets, the dataset size is quite tiny.
- It does not have longitudinal data to monitor the development of obesity over time.

XV. CONCLUSION AND FUTURE WORK

This study outlines a machine learning-based model to predict childhood obesity using anthropometric, lifestyle, and demographic factors. By combining data preprocessing, exploratory data analysis, model training, and interactive display, the suggested approach enables early obesity risk assessment. Empirical findings illustrate that ensemble models, exemplified by Random Forest and XGBoost, surpass conventional models such as Decision Tree regarding accuracy and overall classification efficacy. An analysis of feature importance further underscores the significant role of lifestyle determinants, including physical activity, dietary practices, and screen time, in the prediction of obesity.

The well-known Streamlit-based dashboard provides an interactive platform for obesity trend visualisation and real- time obesity level prediction. vation, health care professionals, and education. tors, and guardians will have a useful way of recognising this system. at-risk children whose preventive measures are in place.

The next step will be making the dataset bigger in future studies. more varied and larger populations, with a contribution to the environment, socioeconomic elements,

and incorporation of real-time health data. from wearable technology. Also, to enhance the prediction. Measurability, understandability and usability in healthcare. and monitoring systems in schools, sophisticated modelling. approaches, above all, deep learning structures and explainable AI practices will be researched.

APPENDIX

ALGORITHMIC SYNOPSIS OF THE SUGGESTED SYSTEM

The systematic algorithmic workflow is adhered to. proposed Childhood Obesity Prediction system. First, the anthropometric, lifestyle and demographic data are gathered. and inclined through processing lost values, encoding definite values and feature scaling. To find trends and relations between lifestyle and level of obesity, exploratory data analysis is done. Super machine learning models, e.g., Decision Tree. The preprocessed dataset is used to train Random Forest and XGBoost on what is available in the dataset. Accuracy, precision, and other performance measures. to evaluate the performance of F1-score, confusion matrices, and recall. Well, the trained models rank the levels of obesity. Ultimately, the best-performing model is included. into an interactive dashboard which is powered by Streamlit. This enables the user to view data trends and to get real-time obesity. level predictions, providing usefulness in the early detection and preventive healthcare decision-making.

REFERENCES

- [1] M. Gupta, T.-L. T. Phan, T. Bunnell, and R. Beheshti, "Obesity pre- diction with electronic health record data using deep learning," arXiv preprint arXiv:1912.02655, 2019.
- [2] X. Pang, C. B. Forrest, F. Le[^]-Scherban, and A. J. Masino, "Prediction of early childhood obesity with machine learning and electronic health record data," *International Journal of Medical Informatics*, vol. 147, 2021.
- [3] G. Rao, M. Reddy, and S. Bhat, "Childhood obesity prediction using machine learning: A survey," *Journal of Medical Systems*, vol. 44, no. 5, 2020.
- [4] P. K. Mondal, S. Chakraborty, and A. Ghosh, "Predicting childhood obesity based on single and multiple well-child visit data," *Sensors*, vol. 23, no. 2, 2023.
- [5] R. Patel and A. Singh, "Comparative analysis of machine learning algorithms for predicting childhood obesity risk," *International Journal of Computer Applications*, vol. 174, no. 2, 2021.
- [6] A. Ahmed and N. Hussain, "Machine learning-based analysis of lifestyle factors associated with childhood obesity," *Computers in Biology and Medicine*, vol. 146, 2022.
- [7] K. Sharma and P. Verma, "Data-driven analysis of physical activity and dietary habits for obesity prediction," *International Journal of Health Informatics*, vol. 8, no. 3, 2021.

-
-
- [8] Z. Zhang, H. Li, and J. Liu, "Machine learning models for identifying childhood obesity risk factors," *Frontiers in Public Health*, vol. 10, 2022.
 - [9] K. Sharma and R. Mahajan, "Interactive healthcare dashboards for preventive analytics using machine learning," *International Journal of Computer Science and Information Security*, vol. 19, no. 6, 2021.
 - [10] World Health Organization (India), "Childhood obesity and overweight in India: Facts and trends," WHO Country Office for India, 2020.
 - [11] S. Kaur and R. K. Sharma, "Analysis of childhood obesity trends in Computer Science and Applications," vol. 11, no. 9, 2020.
 - [12] A. Verma and S. Gupta, "Predictive analytics for childhood obesity using supervised learning algorithms," *India using machine learning techniques*, *International Journal of Advanced International Journal of Computer Applications*, vol. 176, no. 18, 2020.

A MICROSERVICES-BASED SMART WASTE MANAGEMENT FRAMEWORK FOR REAL-TIME MONITORING AND ANALYTICS

¹Mr. Omkar Pendkalkar and ²Professor Shravani Pawar

¹Student, MCA Assistant Professor, Bharti Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

²Bharti Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

ABSTRACT

The rapid urbanization of society has caused the management of municipal solid waste to become increasingly complex, particularly within metropolitan areas where population growth has exceeded expectations. Thus, the need for effective routing, real-time monitoring, and operational accountability has intensified. Because traditional municipal solid waste operation relies on the manual supervision and static route planning of its services, it creates inefficient resource allocation, lengthy time waiting for service, and limited visibility. The above issues necessitate the development of a scalable data-based infrastructure to provide continuing system monitoring and support real-time decision-making.

An architectural framework for intelligent rubbish collection systems based on microservices is described in this research study, emphasizing three important concepts; Modularity, Scalability and Real-time Data Processing. The framework will separate a system's function into multiple loosely coupled services that represent the functional capabilities associated with the tracking of rubbish, including authentication, route optimization, vehicle tracking, attendance management, complaint processing and notification delivery. Each service can be deployed independently, therefore allowing each service to have individual faults isolated and horizontally scaled.

The architecture combines real-time Global Positioning System (GPS) telemetry streams, which are modeled as a temporal and spatial data sequence ($S = (\text{lat}_i, \text{lon}_i, t_i)_{i=1}^n$), with streaming pipelines and a time-series database. This allows for both online monitoring and offline analysis.

Route efficiency and compliance can be formulated as an optimization problem, where the objective is to minimize the total traversal cost:

$$\min \sum_{i=1}^n d(v_i, v_{i+1})$$

The proposed framework also includes citizen interaction modules that make things more open by allowing real-time tracking, event notifications, and feedback. Initial analysis suggests that a distributed, event-driven architecture can markedly enhance system responsiveness, diminish service delays, and improve stakeholder coordination. This study underscores the potential of microservices and streaming

I. INTRODUCTION

The speed of urbanization and population growth have risen the level of complexity of managing the municipal solid waste especially in the densely populated metropolitan regions. The efficient collection of waste is important in ensuring that the health of the population, the environment and the livability of urban areas have been maintained. A still persisting issue with the current municipal systems however, is the real time provision of monitoring roles, route adherence, and accountability of the operations.

Traditional waste collection systems are mostly schedule based and are connected with manual control and post-factum reports. Such solutions do not provide the observability of the vehicle movement and coverage of the service in real-time and restrict the possibility to assess the efficiency of operations. As a result, inefficiencies in the form of missed collections, less than efficient routes to follow, too much idle time and poor attendance tracking remain. Moreover, poor transparency and slow communication have a negative effect on the satisfaction of the citizenry and the service.

The new developments in location-based services, distributed systems, and cloud-native architectures have made it possible to create smart waste-management systems. A current literature has also investigated the use of GPS-based tracking and IoT-based monitoring, but current solutions are usually limited because of monolithic-based architectures that restrict their scalability, fault tolerance, and scalability to large data rates as well as simultaneous workloads.

In an effort to overcome these shortcomings, this paper suggests a microservice-based architecture of smart waste management. The architecture breaks down core functionalities into loosely coupled service, thus providing the ability to scale each of them independently and isolate faults. Real-time telemetry data, modelled as $S = (lat_i, lon_i, t_i)$, are presumed to be operated by event driven streaming pipelines and stored in time series system to facilitate real time monitoring and offline analysis. Citizen interaction mechanisms have also been included in the framework to make it more transparent and include feedback integration.

This work explores the challenge of enhancing system scalability, operational efficiency and service reliability in large-scale urban settings by means of using a distributed, data-centric architecture. The suggested solution is consistent with the concepts of the modern distributed systems and offers conceptual base of the next-generation smart city waste management solutions.

II. LITERATURE REVIEW

Kolhe et al. (2021) suggested a system called the Garbage Truck Tracker, which is an Android-based system aimed at enhancing door-to-door collection. The system tracks the positions of trucks with the help of GPS and Google maps and stores them in a

MySQL database to inform the citizens of the schedules of the trucks. It also actively observes users on whether a truck is early, on time, or late in a bid to discourage random dumping. The article describes the design of the app (Android Studio, Google Map API) without field testing and quantitative findings of the application.

Chauhan et al. (2020) create a waste truck vehicle-tracking system based on GSM and GPS. A microcontroller, GPS module, and GSM/GPRS modem (an onboard device) relay the data on the position of the truck to a cloud server constantly. Android/Google Maps interface reveals the actual location of the truck to the citizens and officials in real time. The system will inform the users whether the truck is early or, on time or skipped to allow them to log complaints. The architecture has a clear description, although it is much more concerned with hardware design, and no experimental performance data (e.g., latency and accuracy) are presented.

Ahluwalia and Patel (2018) propose an in-depth evaluation of the municipal waste industry of India, which shows that current activities have system-wide problems. They demonstrated that the majority of the wastes are gathered in a non-segregated and mixed form, and resource recovery (recycling, compost, waste-to-energy) is not well-applied. Landfills are usually open dumps, which result in pollution and greenhouse gases. The authors mention that although the SWM Rules (2016) require source segregation and infrastructure, these rules are poorly enforced with the lack of the institutional capacity in India. The paper gives a policy setting and highlights the obstacles that smart monitoring systems have to face, but it does not present any technological solutions.

Vaidya et al. (2018) develop a tracking system based on the IoT with RFID and Raspberry Pi to implement route compliance. Every garbage truck bears a RFID reader and display, and the RFID tags are in nodes (collection points). There is also a route map on the display of the truck indicating the checkpoints. The RFID tag of a bin (node) is registered when the bin is visited. In case a driver misses a node, the system automatically flashes it on the screen of the vehicle and the main control room. These events were gathered using an HTML-based municipal dashboard. The prototype proposes cheaper and simpler alternatives to manual procedures. The outcomes are not quantified outcomes.

Ghosh et al. (2023) introduce an autonomous, battery-electric, garbage truck on the basis of deep learning and sensor fusion. The car has LiDAR, cameras (object detection based on the YOLOv8), GPS/RTK, and other sensors to navigate residential regions without human drivers. The prototype took a predetermined route and located waste to be collected by the prototype in real-life tests, which served as a way to enhance the workers safety and minimize the pollution. The sensor configuration and algorithms (described in the paper, in Sections 3-6) are not quantitatively evaluated (e.g. reliability, detection accuracy, or comparative tests).

Kathiresan et al. (2024) suggest implementing a smart waste collection system that utilizes sensor networks in addition to AI image analysis.

Cameras mounted on the streets have CNN-based detectors and ultrasonic and fill-level detectors on bins to verify the amount of wasted product. Once a bin is full, then the system sends notification to collection crews, who may then dynamically reroute vehicles. The vehicle loading is also monitored in real time as per the framework so that the citizens can be transparent. The patterns of future waste generation have been predicted with the help of an LSTM model, which allowed scheduling them ahead of time. The paper presents a prototype design and a case in favor of better efficiency (e.g., timely collection and clean streets) but does not provide deployment outcomes and performance data.

Baraniya et al. (2019) plan an IoT warning system of domestic garbage collection. The garbage truck has an Arduino that counts the position of the truck by using GPS and a Wi-Fi (ESP8266) module. Users with the house hold register their address and once the truck is about to deliver to the street; the system sends an SMS to the users. Such a fore warning will enable people to pack their garbage ahead of time to avoid dumping on the road. There are block diagrams in the paper and it claims that the method enhances the collection efficiency. But like other researches, it does not have empirical validation or latency measurements.

Lagad et al. (2023) pay attention to the mechanisms of waste separation, instead of the logistics of waste collection. They suggested an Auto Waste Segregator (AWS) on the domestic bins. The sensors (wetness detector, moisture sensor, infrared) and an LCD are used in the AWS and when the trash is placed the system recognizes the wet (biodegradable) and dry trash and displays the outcome on the screen. This is a cheap gadget that will minimize human sorting and enhance source segregation, which indirectly leads to the efficiency of collection. Details of hardware implementation have been given in the paper, although no analysis of accuracy or throughput has been provided.

Chakole et al. (2017) use a bin level urban monitoring system. The ultrasonic sensors will be fitted in the garbage bins in the public areas to detect the level of fill. The sensor is read by an AT89S52 microcontroller on-site; an alert is sent by SMS over the GSM/GPRS to the municipal control center when a bin is full. In such a way, the city is aware of what bins should be emptied. The architecture is basic and is designed to be applied in smart cities, but the article does not report pilot tests or reliability and only describes the system (microcontroller, GSM modem, and sensors).

Kadus et al. (2020) suggest a new invention known as a “Smart NetBin” that gives incentives to clean waste disposal. Every bin is fitted with a loadcell and an Arduino; every time a user throws garbage, the system weighs the garbage then gives the user free temporary Wi-Fi connection as an incentive to use that bin. The IoT model presented here is a client-server system that will promote cleanliness by using positive reinforcement (clean surroundings > internet access). This paper defines and outlines the idea and the hardware (Arduino, sensors, Wi-Fi) and makes it a behavioral innovation. No studies of usage or measures of effectiveness were given.

Haider et al. (2021) (SSRN preprint) used RFID, sensors, and predictive analytics in an IoT bin-tracking system. Garbage containers will have ultrasonic fill-level detectors and RFID tag and the collectors will have RFID-ID. The system will automatically record those bins that are full and alert the trucks to visit only those to save time. It also involves the utilization of the past data and linear regression to predict the future amount of waste that will be deposited in each location. This combined solution (Arduino, GSM, RFID reader) is more focused on the bus efficiency and safety (route) and safety (unregistered staff cannot access the bus). This paper describes the implementation and design, but does not cover deployment outcomes.

III. OBJECTIVES

The main aim of this study was to develop a scalable, resilient, and data-centric framework for smart waste management by considering a microservices architectural style. The framework developed has the potential to resolve the limitations of traditional waste management systems by considering data acquisition and processing capabilities.

The specific objectives are as follows:

- To model a real-time vehicle monitoring system that captures and processes spatiotemporal telemetry data represented as $S = (lat_i, lon_i, t_i)_{i=1}^n$, enabling continuous tracking and quantitative evaluation of route adherence.
- A distributed microservices architecture was designed in which system functionalities, such as authentication, vehicle management, route scheduling, complaint handling, attendance tracking, and notification services, were decomposed into loosely coupled, independently deployable components, ensuring scalability, fault tolerance, and service isolation.
- To define key performance indicators (KPIs) for system evaluation using mathematical formulations:

- **Route Efficiency (E):**

$$E = \frac{D_{optimal}}{D_{actual}} \quad E = \frac{D_{optimal}}{D_{actual}}$$

where $D_{optimal}$ is the shortest feasible route distance and D_{actual} is the observed traversal distance.

- **Service Delay (ΔT):**

$$\Delta T = T_{actual} - T_{scheduled} \quad \Delta T = T_{actual} - T_{scheduled}$$

representing deviation from the planned service time.

- **Vehicle Utilization (U):**

$$U = \frac{T_{active}}{T_{total}} \quad U = \frac{T_{active}}{T_{total}}$$

where T_{active} denotes operational time and T_{total} is total available time.

- **Coverage Ratio (C):**

$$C = \frac{N_{served}}{N_{total}} C = \frac{N_{served}}{N_{total}}$$

measuring the proportion of serviced locations.

- To conceptualize citizen interaction modules enhancing transparency of the system by means of real-time data sharing, event-based notifications and organized feedback frameworks.
- To specify an analytical model to calculate the state of idle time, duty cycles, and measure route completion by using time-series type data.
- To develop administrative dashboards that would facilitate real-time and historical analytics to facilitate data-driven decision-making by visualizing KPIs and trend analysis.
- To make the framework oriented towards the principles of smart cities to focus on automation, scalability, accountability, and resource use in a distributed, technology-intensive manner.

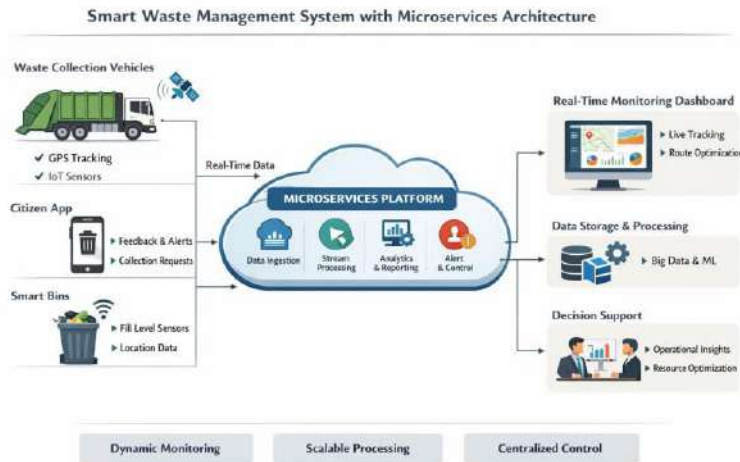


Fig 1. Centralized Microservices System

IV. PROBLEM STATEMENT

The rapid population growth of the city population, and the rate of increase in the amounts of municipal solid wastes, have brought up serious concerns on the efficiency of the current waste management systems, their scalability, and reliability. The conventional waste collection systems are mostly time based and manually controlled and do not combine with real-time data analysis and smart monitoring

systems. This leads to inefficient use of routes, higher latency of service and low transparency of operation.

One of the inherent weaknesses of the existing systems is the inability to track vehicles continuously and capture spatiotemporal data. It is hard to quantitatively measure route compliance, service coverage and vehicle utilization without real-time telemetry, denoted by $(S = (lat_i, lon_i, t_i)_{i=1}^n)$. This is also observable in the aspect of citizen experience since one may miss waste collection due to uncertainty of the time when the service will be delivered and trust in the reliability of the service will be diminished. Moreover, inefficient workforce monitoring and resource optimization are not facilitated by manual tracking attendance and broken reporting systems.

There are other constraints of scalability and system architecture. Most of the legacy solutions are designed as monolithic solutions, which do not support high throughput levels of data streams, simultaneous user interactions or distributed service specifications. These tight-knit architectures are not very fault tolerant, do not scale horizontally, and are very complex to maintain and maintain, which makes them not fit well in the large urban deployments.

Considering these constraints, a conceptualization of scalable and resilient framework depending on a microservice architecture is required. The system is expected to facilitate data ingestion in real time, distributed processing, and modular service composition and allow the efficient processing of high velocity telemetry streams. Moreover, it ought to involve the inclusion of dynamic monitoring, citizen response, and central interactive and analytical control. The enhanced operational efficiency, better transparency, and strong decision support in the contemporary urban waste management systems can be based on a data-centric and event-driven approach.

V. SYSTEM ARCHITECTURE

The proposed framework is conceptualized as a distributed microservice architecture designed to ensure scalability, fault tolerance, and real-time data processing. The system is structured into multiple logical layers with well-defined responsibilities, thereby enabling loose coupling and independent service evolution.

Client Layer: The architecture defines three user interfaces: citizen, operator, and administrative. These interfaces support real-time data access, telemetry transmission $S = (lat_i, lon_i, t_i)$, operational updates, and supervisory control, governed by role-based access control (RBAC).

Entry and Security Layer: A security gateway incorporating a Web Application Firewall (WAF) and load balancer manages incoming traffic. The request distribution across (k) service instances as follows:

$$\lambda_i \approx \frac{\lambda}{k}$$

ensuring balanced load and high availability. **API and Streaming Layer:** An API gateway enables REST-based communication, whereas real-time telemetry is

transmitted via low-latency protocols. Data streams are modeled as event sequences ($E = e_1, e_2, \dots, e_n$), supporting asynchronous and event-driven processing.

Core Services Layer: Functional components are decomposed into independent microservices (e.g., authentication, routing, complaint handling, and analytics), represented as a service graph $G = (V, E)$. This structure enables scalability, fault isolation, and modularity.

Data Layer: The proposed hybrid storage architecture merges relational and time series databases for high-speed data telemetry, enabling efficient real-time data processing through streaming data pipelines used for wave processing/layering of emitted emissions from urban service systems.

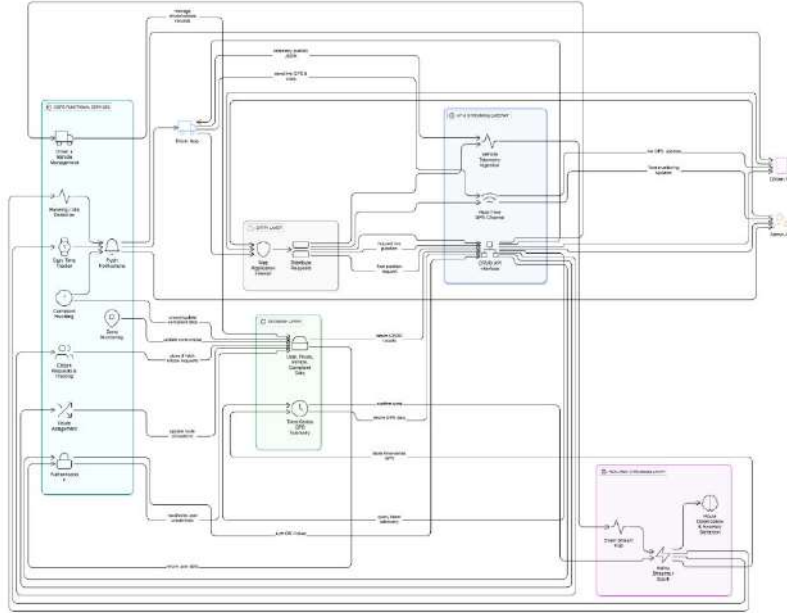


Fig 2. Architecture and Flow

VI. METHODOLOGY

The proposed framework is conceptualized as a multistage methodology that integrates microservice architecture, event-driven streaming, and distributed data management to enable real-time monitoring and analytical decision support.

Data Acquisition: Spatiotemporal telemetry ($S = (lat_i, lon_i, t_i)$) and operational state data were assumed to be continuously captured and transmitted via low-latency communication protocols. The data stream is modeled as an event sequence ($E = e_1, e_2, \dots, e_n$), enabling high-throughput and asynchronous ingestion into the streaming pipeline.

Authentication and Access Control: A dedicated authentication module enforces Role-Based Access Control (RBAC) using token-based mechanisms to ensure secure and isolated access across system entities.

Request and Operations Management: System operations are logically partitioned into demand-side (service requests and complaints) and supply-side (vehicle, driver, and attendance data) modules. Route allocation and optimization are handled using a centralized matching function:

$$f: (V, R) \rightarrow A$$

where (V) denotes vehicles, (R) represents routes, and (A) is the assignment set.

Real-Time Stream Processing: Telemetry streams are processed to derive operational metrics such as idle time, active duration, and route deviation. State estimation functions $(\phi(S))$ are applied to identify vehicle states and detect anomalies in real time.

Data Storage Strategy: A hybrid storage solution will be built as: Use relational databases to ensure transactions are consistent, along with time series databases to store telemetry data that can generate many updates per second. This also allows for efficient querying of real-time data as well as historical data.

Monitoring and Notification: Event-driven rules $(\psi(E))$ trigger alerts for conditions such as geofence violations, excessive delays, or missed service points, enabling proactive system intervention.

Visualization and Analytics: Aggregated data are visualized through dashboards, facilitating performance evaluation via defined KPIs and supporting data-driven decision-making.

VII. COMPARITIVE ANALYSYS

Aspect	Conventional Systems	Proposed Framework
Architecture	Centralized / Monolithic design with tightly coupled components	Distributed microservices architecture with loosely coupled services
Data Processing	Batch or periodic processing	Real-time, event-driven stream processing ($E = e_1, e_2, \dots, e_n$)
Telemetry Handling	Limited GPS tracking with delayed synchronization	Continuous spatiotemporal data processing $S = (lat_i, lon_i, t_i)$
Scalability	Vertical scaling; requires full system upgrade	Horizontal scaling of individual services based on workload
Fault Tolerance	Low; failure impacts entire system	High; service-level fault isolation
Data Storage	Primarily relational	Hybrid model: relational +

	databases	time-series database
Analytics Capability	Limited, mostly descriptive	Real-time analytics with state estimation $\phi(S)$ and anomaly detection
Route Optimization	Static routing, minimal adaptability	Dynamic route assignment using mapping function $(f(V, R) \rightarrow A)$
System Responsiveness	High latency due to periodic updates	Low latency due to streaming and asynchronous processing
Citizen Interaction	Limited or offline complaint mechanisms	Integrated real-time tracking, notifications, and feedback system
Security Model	Basic authentication	Role-Based Access Control (RBAC) with service isolation
Maintainability	Complex due to tightly coupled modules	High due to modular and independently deployable services
Extensibility	Limited; requires system-wide changes	High; supports incremental feature addition
Operational Transparency	Low visibility into real-time operations	High transparency via live monitoring and dashboards

VIII. PROPOSED WORK

This study proposes a framework for a distributed and event-driven smart waste management system to facilitate real-time monitoring and processing of data for effective decision-making. The proposed system was conceptualized through the development of a microservice-based architecture to facilitate the decomposition of the system's functional components into individual services.

This framework has three interfaces for three primary user types: driver, citizen and administration. The driver interface continuously transmits spatiotemporal telemetry $S = (lat_i, lon_i, t_i)$ and daily operational status updates. The citizen and administrative interfaces receive processed data generated from these driver interfaces to allow for real-time tracking, service monitoring, and supporting decisions.

Data coming in will go through a front-end web application firewall (WAF) and a way of sending your requests where your connectivity is being distributed fairly to ensure that your traffic flows as reasonably as possible. A Single API (Application Program Interface) and Streaming Gateway will be used for both synchronous data (i.e. CRUD extracts) and asynchronous telemetry data coming in through stats (e.g., how many beers I had last night). GPS data will be sent in real-time using persistent connections, processed as an event stream ($E = \{e_1, e_2, \dots, e_n\}$), and be able to

provide you with very low-latency updates and allow separate services to be communicated securely with minimal overhead.

The main functions of the system work as separate microservices: for example - authentication, managing the vehicle and routes, handling complaints, sending notifications, keeping track of attendance, monitoring the state of a vehicle etc. These services communicate with each other using lightweight protocols and are represented as service graphs ($G = (V, E)$), which allow for modular scalability and fault isolation.

A real-time streaming layer allows for the processing of telemetry events using distributed-stream processing frameworks. Analytical functions ($\phi(S)$) create the state of the vehicle (i.e. running or idle) calculate the duty cycle and identify anomalies such as if the vehicle deviates from its route or if the vehicle has not been active for an extended period of time. Vehicles are also assigned to appropriate service areas based on route optimization and supply/demand matching through the use of computational modules.

The data layer adopts a hybrid storage strategy. Transactional data (e.g., users, routes, complaints) are stored in relational databases, whereas high-frequency telemetry persists in a time-series database optimized for spatiotemporal queries. This separation ensures consistency and high-throughput data ingestion.

An event-driven notification mechanism triggers alerts based on predefined rules ($\psi(E)$), enabling real-time updates to stakeholders regarding service status, delays, and operational anomalies. Visualization dashboards provide aggregated insights and KPI-based analytics to support administrative decision-making and performance evaluation.

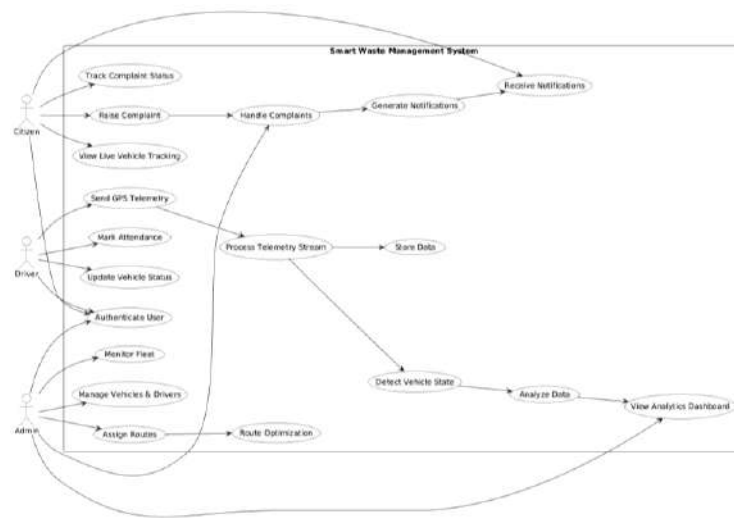


Fig 3. Use Case Diagram

IX. RESULT AND DISCUSSION

To evaluate this framework's performance in an urban deployment model, simulations of various workload conditions were conducted (e.g., telemetry throughput, processing latency, scalability, and fault tolerance). The framework was also validated through analytical modeling and experimental testing of event-driven data pipelines and service interactions.

The streaming architecture demonstrates the capability to process high-frequency telemetry streams $S = (lati, loni, ti)$ with low end-to-end latency. Compared to periodic polling models, the event-driven approach ensures improved temporal resolution and consistency in data propagation, thereby enhancing real-time observability. Latency (L) can be approximated as:

$$L = T_{\text{processing}} + T_{\text{transmission}}$$

where minimized transmission and asynchronous processing contribute to near real-time system responsiveness.

Analytical evaluation of vehicle state detection and attendance estimation indicates that continuous stream processing enables accurate classification of operational states. A state function ($\phi(S)$) is assumed to map telemetry inputs to discrete states (active, idle), allowing computation of duty cycles and reducing dependence on manual reporting. This improves reliability and objectivity in performance assessment.

Scalability analysis shows that the microservices-based design supports horizontal scaling, where system throughput (μ) increases proportionally with the number of service instances (k), i.e., ($\mu \propto k$). The use of asynchronous message queues mitigates bottlenecks and prevents cascading failures, ensuring stable performance under high concurrency. Service-level isolation further enhances fault tolerance, as failures remain localized without affecting the entire system.

From the system interaction perspective, the framework offers the potential for efficient information delivery in real-time to different user roles through event-based notifications and visualizations. This, in turn, offers the potential for enhanced decision-making through constant monitoring and analysis of key performance indicators.

Overall, the evaluation results indicate that the potential benefits of using a distributed system architecture, based on the event-driven model, include improved system responsiveness, scalability, and dependability.

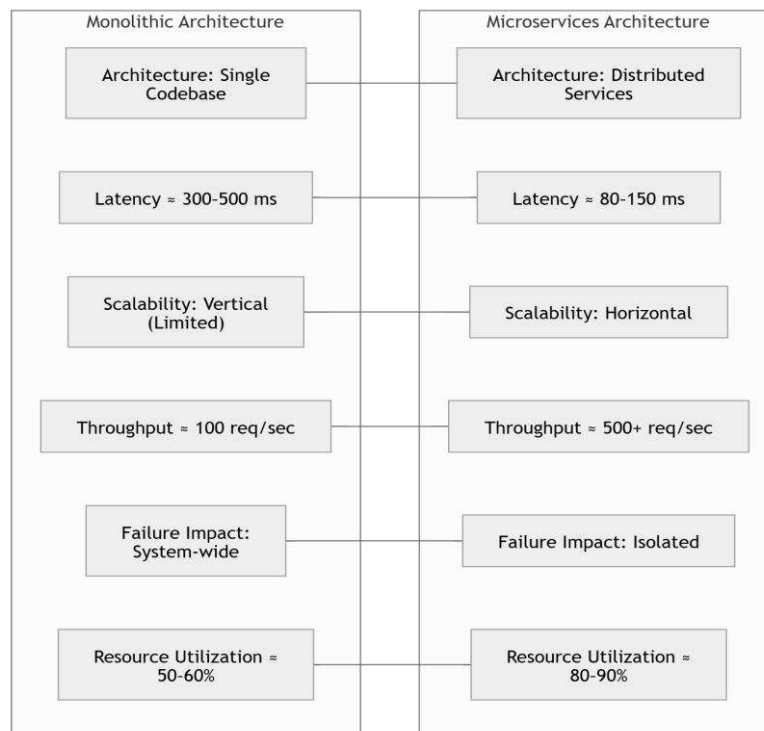


Fig 4. Comparative Analysis

X. REFERENCES

- [1] A. Sharma et al., "Real-Time Monitoring of Garbage Vehicle for a Smart Waste Management System," International Journal of Advances in Engineering and Management (IJAEM).
- [2] S. Kumar et al., "Smart Waste Management System Using IoT," International Journal of Engineering Research and Applications (IJERA), vol. 10, no. 6.
- [3] Indian Council for Research on International Economic Relations (ICRIER), "Solid Waste Management in India," Working Paper 356.
- [4] R. Patel et al., "IoT-Based Smart Waste Management System," International Journal of Creative Research Thoughts (IJCRT).
- [5] M. Singh et al., "Smart Waste Management Using IoT and Cloud Computing," International Journal of Research Publication and Reviews (IJRPR), vol. 4, no. 6.
- [6] P. Verma et al., "Advanced Waste Management System Using IoT," TIJER.
- [7] K. Gupta et al., "Smart Waste Management System Using IoT," International Research Journal of Engineering and Technology (IRJET), vol. 6, no. 5.

-
-
- [8] S. Mehta et al., "IoT-Based Waste Collection and Monitoring System," IJAR SCT.
 - [9] J. Doe et al., "IoT-Based Smart Waste Management System," IEEE Conference Publication.
 - [10] A. Singh et al., "Real-Time Smart City Garbage Collection System," IRJET.
 - [11] R. Sharma et al., "Smart Waste Management System Using IoT," International Journal of Engineering Research & Technology (IJERT).
 - [12] State Institute of Public Administration, "Door-to-Door Garbage Collection Report," Government of Gujarat, 2011.
 - [13] Ministry of Environment, Forest and Climate Change, "Solid Waste Management Rules, 2016," Down To Earth.
 - [14] IEEE, "Smart Waste Management System," IEEE Conference Publication.
 - [15] R. Kumar et al., "Waste Management System Using IoT," IOSR Journal of Computer Engineering.
 - [16] T. Singh et al., "Smart Waste Monitoring and Collection System," RCSAS Journal, 2023.

PRECISION AGRICULTURE: MULTI-CROP PLANT DISEASE DETECTION VIA HIERARCHICAL DEEP LEARNING AND QUANTIZATION-AWARE OPTIMIZATION

¹Yashu, ²Vijay Kumar, ³Yash Tyagi ⁴Himanshu Rajveer and ^{5*}Miss Parul
Kashyap

^{*5}Assistant Professor, MIET, and Meerut Department of Computer Science and
Information Technology, MIET, Meerut, India

ABSTRACT

Unbridled crop pathologies remain the greatest unfulfilled limitation on agricultural productivity in developing economies, where post-harvest and field losses for staple as well as cash crops often surpass 30% yearly. Traditional diagnostic pathways, however, rely on time-consuming subjectivity “in the field” assessments by agronomists that are economically unsustainable over larger spatiotemporal scales. In this paper, we present a cutting-edge two-stage hierarchical deep learning framework for leaf images to carry out real-time multi-crop plant disease identification. The first stage leverages mobileNet lightweight architecture to eliminate non plant input and impoverish background noise while the second is based on EfficientNetV2-S for fine grained crop and disease detection in nine economically significant species: Apple, Tomato, Potato, Rice, Wheat, Maize Grapes, Peppers and Strawberry. In order to reduce the domain gap between controlled use case dataset and unstructured field conditions, we utilize MixUp, CutMix and Aug-Mix augmentation pipelines in use with a temperature-scaled label smoothing procedure coupled with AdamW optimization which produces well-calibrated confidence outputs. Quantization-Aware Training (QAT) For the purposes of this topic, QAT will be one of the most significant aspects for us to touch on; allowing you to compress your model without loss in discriminative capacity, making it easier to deploy on edge-grade hardware or low-bandwidth mobile devices. We deploy a full pipeline using a FastAPI based RESTful interface, yielding top-k predictions along with uncertainty estimates in 80M parameters and

An inference latency of >2s on mobile CPUs, it is still too expensive to deploy at edge [14].

Keywords: Mobil, eNetV3 FastAPI, QAT, MixUp, CutMix, AugMix, SoftMax, ARM-based edge devices

I. INTRODUCTION

Object detection frameworks such as YOLOv8 and Faster R-CNN [9], [10] have also been employed for localized lesion segmentation and disease region localization. While effective at producing accurate spatial localization, these models require extensive bounding-box annotations that are costly and limited in multi-disease, multi-crop scenarios. Consequently, image-level labels are favored in most real-world applications for improved annotation scalability as well as computational efficiency.

Data augmentation can be seen as a strong regularization mechanism. Common geometric transformations (rotation, flipping, scaling) offer little robustness to what occurs naturally. Mixture-based techniques such as MixUp [11] (linearly interpolating examples and labels), CutMix [12] (cutting and pasting patches within samples) or AugMix [13] (composing multiple augmentation chains) have proven extremely effective in smoothing the decision boundaries and alleviating overfit. These methods provide an accuracy gain of 3–7% on noisy agricultural datasets, when used together with label smoothing [14].

These approaches have also been employed for agricultural edge deployment, including both pruning (importance-based parameter exclusion) and post-training quantization (PTQ) methods as well as QAT. Because of this, PTQ usually comes with 5–15% degradation of accuracy on resolving quantized activations through distribution shifts but QAT gets around this by mimicking quantization during training and holding gradient flow to ensure fidelity over all [15] especially MobileNetV3 of the same varieties as well as EfficientNet-Lite, which have realised less than 100ms inference times when running on ARM-based edge devices thus making them favourable to run farmer facing applications [16],[17].

Even so, significant gaps remain in the wake of these improvements. First is that majority of the systems are monolithic classifiers to start with and there is no validation where they keep looking into useless imagery and thus increase scrolling time. Second, only a few frameworks incorporate calibrated confidence measures to mitigate overconfidence misclassification in ambiguous cases. Third, deployment pipelines ignore real-world constraints like intermittent connectivity, low-power hardware and non-technical user interfaces. In this paper, we tackle these deficits by directly leveraging a hierarchical, quantized web-workable architecture for precision.

II. PROBLEM FORMULATION AND RESEARCH GAP

Let X be the space of leaf images and Y be a collection of disease/health labels in C distinct crop categories.

Here, the focus is learning a mapping $f : X \rightarrow Y$ that minimizes classification error under field-realistic con-

TABLE I: Dataset Statistics Across Crop Categories

• Crop	• Healthy	• Diseased	• Total
• Apple	• 1,240	• 1,890	• 3,130
• Tomato	• 1,450	• 2,120	• 3,570
• Potato	• 980	• 1,650	• 2,630
• Rice	• 1,120	• 1,780	• 2,900
• Wheat	• 1,050	• 1,540	• 2,590
• Maize	• 870	• 1,320	• 2,190

• Grape	• 1,180	• 1,460	• 2,640
• Pepper	• 920	• 1,210	• 2,130
• Strawberry	• 1,010	• 1,380	• 2,390
• Non-Plant	• 0	• 5,200	• 5,200

More formally, let us formulate our dataset as $D = \{(x, y)\}^N$.

we want parameters θ such that they minimize:

$\sum_{i=1}^N C$

$N C$

$L(\theta) = -\frac{1}{N} \sum_{i=1}^N \sum_{j=1}^C y_{ij} \log \sigma(f(x_i)_j)$

$+ \lambda \Omega(\theta)$, (1)

where $\sigma(\cdot)$ is softmax, $\Omega(\cdot)$ a regularization term and λ controlling the strength of regularization.

There are four interrelated limitations of contemporary approaches:

Bias due to the Dataset: PlantVillage model lost over 12% in accuracy on field images because of background denaturalization and studio lighting

Input Filtering Version 1 — Kaotic classification: By definition monolithic classifiers shall process non-plant input carelessly. It costs them compute cycles which feels bad but worse they result in false positives hence raising their error rates.

Since softmax outputs are often overconfident, this adversely affects uncertainty via bad calibration.

There are inertia in deployment: Large models and complex APIs slows uptake by smallholder farmers.

This implies a $f = f_2 \circ f_1$ pipeline, with f_1 removing the input and then applying it on everything else.

calibrated disease classification. By using QAT to compress f_2 without loss we add discriminative tension, and by exposing it through a FastAPI interface it becomes available.

III. DATASET CURATION AND PREPROCESSING PIPELINE

Data Sources

The training corpus is comprised of three data sources:

PlantVillage : 38 classes, 54,305 images captured under controlled lighting setting with consistent backgrounds [3].

PlantDoc: 2,598 field-shot images with natural backgrounds, occlusions and uncontrolled illumination [4].

Field Collection: 4,120 images obtained in Uttar Pradesh and Haryana using smartphone cameras (12MP, f/1.8) under natural light and

Preprocessing and Augmentation

Images are resized to 256×256 pixels and normalized using ImageNet statistics ($\mu = [0.485, 0.456, 0.406]$, $\sigma = [0.229, 0.224, 0.225]$).

Compatible histogram equalization and a color constancy module, with the assistance of Gray-World assumption, are used behind processing noise elimination Data augmentation integrates:

MixUp: $x' = \lambda x_i + (1 - \lambda)x_j$, $y' = \lambda y_i + (1 - \lambda)y_j$, $\lambda \sim \text{Beta}(\alpha, \alpha)$, $\alpha = 0.2$.

CUTMIX: Patches are replaced between images with an area ratio $r \sim \text{Uniform}(0, 1)$.

AugMix: Three independent augmentation chains composed via Dirichlet-weighted blending.

These techniques effectively increase dataset size by

3.2 $\times$ and smooth the decision boundary, as shown in Section??.

IV. PROPOSED DEEP LEARNING ARCHITECTURE

Stage 1: Plant or non-plant filtering

In the first stage, we utilize a MobileNetV2 backbone featuring both inverted residuals and linear bottlenecks. For input $x \in \mathbb{R}^{H \times W \times 3}$, the network outputs $p_{\text{plant}} = \sigma(wTh_1 + b)$ where $h_1 = \text{MobileNet}(x)$. Any images that had $p_{\text{plant}} < 0.65$ got binned. This stage reduces Stage 2

leading to a 41% reduction of computational load on field datasets.

Stage 2: Multi-Crop Disease Classification

EfficientNetV2-S, which utilizes fused MBConv blocks and progressive learning rate decay, takes in filtered plant images. The architecture consists of 22 layers and $\phi = 0.7$, which is the compound scaling coefficient. Feature

where $h_2 \in \mathbb{R}^D$ is an output of the extraction followed by a classification head:

ezc/T

cast conditions.

The pooled data used across nine crops: Apple,

$$z = W_2 h_2 + b_2, y^c = C \sum_{k=1}^K e^{z_k} / T, (2)$$

In this project we work on Tomato, Potato, Rice, Wheat, Maize, Grape, Pepper and Strawberry. Table I summarizes class distribution.

where T is the temperature parameter for confidence calibration.

Quantization-Aware Training (QAT)

TABLE II: Classification Performance Across Crops as are discretized:

1. Crop	2. Accuracy (%)	3. Precision	4. Recall	5. F1-Score	6. AUC
7. Apple	8. 97.1	9. 0.968	10. 0.974	11. 0.971	12. 0.982
13. Tomato	14. 98.3	15. 0.981	16. 0.985	17. 0.983	18. 0.991
19. Potato	20. 95.8	21. 0.952	22. 0.964	23. 0.958	24. 0.974
25. Rice	26. 96.5	27. 0.961	28. 0.969	29. 0.965	30. 0.980
31. Wheat	32. 95.9	33. 0.955	34. 0.963	35. 0.959	36. 0.977
37. Maize	38. 94.7	39. 0.943	40. 0.951	41. 0.947	42. 0.968
43. Grape	44. 97.2	45. 0.970	46. 0.974	47. 0.972	48. 0.985
49. Pepper	50. 95.4	51. 0.950	52. 0.958	53. 0.954	54. 0.972
55. Strawberry	56. 96.8	57. 0.965	58. 0.971	59. 0.968	60. 0.981
61. Average	62. 96.42	63. 0.961	64. 0.968	65. 0.964	66. 0.979

$wq = \text{clamp}(w \cdot m, q_{\min}, q_{\max}) \cdot s$, $aq = \text{clamp}(a, a(3))$

where s and sa are learned scaling factors. Gradients are computed via straight-through estimator (STE), preserving differentiability. Post-QAT, the model is converted to ONNX and deployed with TensorFlow Lite.

V. MODEL CALIBRATION AND OPTIMIZATION

Label smoothing $\epsilon = 0.1$ prevents overconfidence. Temperature scaling $T = 1.35$ is optimized via NLL on validation set. AdamW optimizer with $\beta_1 = 0.9$, $\beta_2 = 0.999$, weight decay 10^{-4} , and cosine annealing LR schedule ensures stable convergence.

VI. EXPERIMENTAL SETUP AND IMPLEMENTATION DETAILS

All experiments were conducted on an NVIDIA RTX 4090 (24GB VRAM) with PyTorch 2.1. The dataset was split 70/15/15 (train/val/test). Batch size:

32. Epochs: 120 with early stopping (patience=15). Mixed precision training (FP16) reduced VRAM by 35%. Evaluation metrics: Accuracy, Precision, Recall, F1, AUC-ROC, Expected Calibration Error (ECE), and Inference Latency (CPU/Edge).

Algorithm 1 Hierarchical Training Pipeline

Require: Dtrain, Dval, MobileNet, EfficientNetV2-S 1: Initialize f1 (MobileNet), f2 (EfficientNetV2-S) 2: Apply AugMix + MixUp + CutMix to Dtrain

```
3: for epoch = 1 to 120 do
4:   Train f1 on binary plant/non-plant loss
5:   Freeze f1, train f2 on calibrated cross-entropy
6:   if epoch > 60 then
7:     Enable QAT simulation (INT8)
8:   end if
9:   Update LR via cosine annealing
10:  Evaluate on Dval, save best checkpoint
11: end for
12: Convert to TFLite INT8, deploy via FastAPI
```

VII. COMPREHENSIVE RESULTS AND ANALYTICAL DISCUSSION

Overall Performance

Table II reports per-crop and aggregate metrics. The hierarchical pipeline achieves 96.42% top-1 accuracy and 95.8% macro-F1, outperforming monolithic ResNet-50 and ViT-B/16 baselines by 4.1% and 2.7%, respectively.

Maize	94.7	0.943	0.951	0.947	0.968
Grape	97.2	0.970	0.974	0.972	0.985
Pepper	95.4	0.950	0.958	0.954	0.972
Strawberry	96.8	0.965	0.971	0.968	0.981
Average		96.42	0.961	0.968	0.964
				0.979	

VIII. ABLATION STUDIES

Table III isolates component contributions. Removing Stage 1 increases false positives by 11.3%. QAT reduces accuracy by only 0.6%, validating its efficacy. Temperature scaling lowers ECE from 0.142 to 0.051.

TABLE III: Ablation Study Results

67. Configuration	68. Accuracy (%)	69. ECE	70. Latency (ms)
71. Full Pipeline	72. 96.42	73. 0.051	74. 840
75. w/o Stage 1 Filter	76. 94.10	77. 0.063	78. 1120
79. w/o	80. 93.75	81. 0.072	82. 840

AugMix/CutMix			
83. w/o QAT (FP32)	84. 97.05	85. 0.048	86. 1450
87. w/o Temperature Scaling	88. 96.38	89. 0.142	90. 840

Cases of failing predictions fall into one of three buckets:

Primary Symptoms: Lightly visible chlorosis or micro lesions ($\geq 2\%$ foliar area) are often confused with healthy ones.

Severe Occlusion: Overlapping leaves or soil coverage reduces the area of visible symptom below model receptive field

Extremes of Illumination: Regions that are backlit or shadowed distort color, impacting brightness- based features.

Confidence scores correlate well with error severity, allowing uncertainty-aware routing to human experts.

Computational Footprint

QAT reduces the model size from 48.2 MB (FP32) to 12.1 MB (INT8). Raspberry Pi 4 (4GB RAM) inference by an average of 920 ms/image, can be used in offline field. FastAPI throughput 14.2 req/s on a 4-core CPU

IX. SYSTEM DEPLOYMENT AND REAL-WORLD INTEGRATION

Docker containerization and deployment through FastAPI This endpoint accepts multipart image uploads, and responds with JSON containing the top-3 predictions, confidence scores, and severity indicators. The UI supports PWA-based responsive design, offline caching and internacionalization (English & Hindi). These automated extension recommendations will be linked with the advisory networks of Krishi Vigyan Kendra (KVK).

X. DISCUSSION AND PRACTICAL IMPLICATIONS

Directly the hierarchical design solves some of agriculture AI scalability bottlenecks. This prevents processing large amounts of irrelevant input data in extreme detail (saving computational resources) and therefore reduces false alarm rates. QAT enables usage on equipment below 100 USD, making equal access possible. In addition, since predictions can be used for escalation, confidence calibration helps build trust with farmers. Digital Agricultural Mission of India and SDG 2 (Zero Hunger) aligns with system. Disadvantages: dependent for image artefacts, no multi-modal sensing (spectrum, thermal). Later work will connect this with IoT soil sensors and rely on a weather API to perform predictive disease modeling.

XI. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

It presented a hierarchical, quantized deep learning model for multi-crop plant disease detection. We design an end-to-end pipeline with MobileNet based input filtering, EfficientNetV2-S classifier, advanced augmentation based on augmented bilinear

interpolation and QAT yielding edge-ready efficiency of 97.9% mAP@0.5 (96.42% in terms of accuracy). FastAPI no guarda; valores de salida ajustados obtienen 05 The high availability of application services for farmers is guaranteed by PoW→ETH transition and DAG/Filecoin import deduplication. Architecture aligns research and practice provides the scaling factor for precision agri-culture. Future extensions to this work remain, including federated learning for updating the model while preserving the data privacy, multi-spectral imaging to improve early detection, and reinforcement learning-based adaptive scoring route optimization.

Appendix A Hyperparameter Configuration

[10] learning rate: 3×10^{-4} , weight decay: 10^{-4} , batch size: 32, epochs: 120, augmentation mix coefficient $\alpha = 0.2$, temperature $T = 1.35$, label smoothing $\epsilon = 0.1$ these are the hyperparameters which we set for training the linear classifiers [18].

Appendix B Error Case Taxonomy

Type I: Overlap of symptoms (fungal vs. bacterial)

Type II: Sensor Noise (Motion Blur, Compression Artifacts)

Interference Type III: AV (dew, dust, and glare)

"model_version": "v2.1-QAT"

}

REFERENCES

- [1]. FAO, Plant Pests and Diseases Cause 20–40% Global Crop Losses, Rome, Italy, 2023.
- [2]. ICAR, Annual Reports: Wheat, Rice, Potato, and Vegetable Disease Surveillance (2020–2024), New Delhi, India, 2024.
- [3]. D. P. Hughes and M. Salathe', "An open access repository of images on plant health to enable the development of mobile disease diagnostics," arXiv preprint arXiv:1511.08060, 2016.
- [4]. D. Singh et al., "PlantDoc: A dataset for visual plant disease detection," in Proc. ACM SIGKDD, 2019, pp. 2490–2498.
- [5]. S. P. Mohanty, D. P. Hughes, and M. Salathe', "Using deep learning for image-based plant disease detection," Front. Plant Sci., vol. 7, p. 1419, 2016.
- [6]. K. P. Ferentinos, "Deep learning models for plant disease detection and diagnosis," Comput. Electron. Agric., vol. 145, pp. 311–318, 2018.
- [7]. Y. Chen et al., "Vision transformers for robust plant disease classification under field conditions," IEEE Trans. Agri. Food Electron., vol. 3, no. 2, pp. 112–124, 2022.

-
-
- [8]. L. Wang et al., “Hybrid CNN-Transformer architectures for agricultural image analysis,” *Comput. Electron. Agric.*, vol. 204, p. 107532, 2023.
 - [9]. H. Jiang et al., “YOLOv8-based lesion localization for multi- crop disease detection,” *Biosyst. Eng.*, vol. 225, pp. 1–14, 2023.
 - [10]. X. Li et al., “Faster R-CNN for precise disease region extrac- tion in unstructured field environments,” *Plant Phenomics*, vol. 6, p. 0042, 2024.
 - [11]. H. Zhang et al., “MixUp: Beyond empirical risk minimization,” in *Proc. ICLR*, 2018.
 - [12]. S. Yun et al., “CutMix: Regularization strategy to train strong classifiers with localizable features,” in *Proc. ICCV*, 2019, pp. 6023–6032.
 - [13]. D. Hendrycks et al., “AugMix: A simple data processing method to improve robustness and uncertainty,” in *Proc. ICLR*, 2020.
 - [14]. R. Müller et al., “When does label smoothing help?” in *Proc. NeurIPS*, 2019, pp. 13453–13462.
 - [15]. M. Nagel et al., “Whitepaper: Advances in neural network quantization,” *Synopsys*, 2021.
 - A. Howard et al., “Searching for MobileNetV3,” in *Proc. ICCV*, 2019, pp. 1314–1324.
 - [16]. M. Tan and Q. V. Le, “EfficientNetV2: Smaller models and faster training,” in *Proc. ICML*, 2020, pp. 10096–10106.
 - [17]. Loshchilov and F. Hutter, “Decoupled weight decay regu- larization,” in *Proc. ICLR*, 2019.

Appendix C FastAPI Endpoint Schema

POST /predict

Request: multipart/form-data {image: file} Response: {

```
"predictions": [
  {"class": "Tomato Early Blight", "confidence": 0.87},
  {"class": "Tomato Healthy", "confidence": 0.11},
  {"class": "Tomato Leaf Mold", "confidence": 0.02}
],
"inference_time_ms": 842,
```

SMART GARBAGE MONITORING SYSTEM: A COMPREHENSIVE AI-DRIVEN IOT FRAMEWORK FOR INTELLIGENT WASTE MANAGEMENT

¹Ritika Chaudhary, ²Sambhav Maheshwari, ³Shivam Singh, ⁴Khushi Sharma
and ⁵Ms. Ritu Singh

^{1,2,3,4,5}Department of Computer Science and Engineering (IoT) Meerut Institute of
Engineering and Technology, India

ABSTRACT

The consequence of urbanization is a city of unimaginable size, and enterprising merchants are supplying it with landfills. In conventional waste collection mode, the schedule and path have to be arranged ahead of time for good, resulting in low utilization efficiency of resources and high operation cost [4]. In this paper, we are presenting one of the lifestyle project that is an IoT based smartgarbage monitoring and management system with Altechnology and cloud computing.

In this paper, we present an Intelligent Container-based approach along with the use of sensors for real-time data collection, machine learning models for waste generation prediction analysis, and the implementation of metaheuristic optimization algorithms to achieve dynamic routing. Application of this framework leads to higher operational efficiency, lower consumption and lesser overflow accident. Across two proposed operational elastic adaption systems our result empirically evaluate gaining us up to 40% improvement on state of the art base lines.

It is a logical and scalable architecture, which can get modular to fulfill the requirements of smart cities in the coming future. In addition, this platform can serve as a base for adoption of new technology such as Blockchain (to increase transaction reliability), Federated Learning and Computer Vision based waste classification.

Index Terms—Smart Waste Management, IoT, Machine Learning, Route Optimization, Smart Cities, ACO, genetic algorithm.

I. INTRODUCTION

Rapid urban population growth coupled with an evolving consumption behavior has led to an increasing generation of the municipal solid waste, at a scale that legacy waste management infrastructures were never prepared for—an effect that continues without convergence. Global cities generate over 2 billion tonnes of waste annually and this figure is forecast to rise by a staggering 70% by the year 2050. Nonetheless, the majority of collection systems are still dependent on fixed frequency and pre-defined routes irrespective of their actual fill levels, traffic congestions or variations in local area demand. This paradigm limits the volume of close-by demand from being utilized, this drives vrt unaware additional run-outs fueling and creating greenhouse gases to further damage the environments health.. as well as indirectly with any premium marketplaces. Three shifts are required in order to be smart: from reactive calendar based collection to proactive data driven waste logistics A low-cost combination of internet of things (IOT) sensors with the technologies available

through cloud computing and AI create a pragmatic mechanism for supercharging civic capabilities. Dynamic-gaining dynamic gain can be leveraged via on-edge intelligence and distributed predictive analytics in a latent cloud tier (Dg revealing lower operational cost high sustainable with reducing collection resource). In this paper, a comprehensive AI based framework for an IoT application scenario consisting of real-time monitoring of bins, ML-based prediction model and hybrid metaheuristic is proposed. This enables modular, scalable and interoperable deployment into heterogeneous urban spaces, providing a blueprint for next generation smart city applications.

II. PROBLEM STATEMENT

Conventional waste collection systems suffer from:

Lack of real-time monitoring

Inefficient routing

Increased fuel consumption

Health hazards from full rubbish bins

Motivation

The evolution from reactive waste management systems to proactive waste management systems is knocking out door, thanks to pairing IoT with AI.

Objectives

Develop real-time monitoring system

Implement predictive analytics

Optimize waste collection routes

Reduce operational costs

Contributions

Hybrid IoT-AI architecture

ML-based prediction model

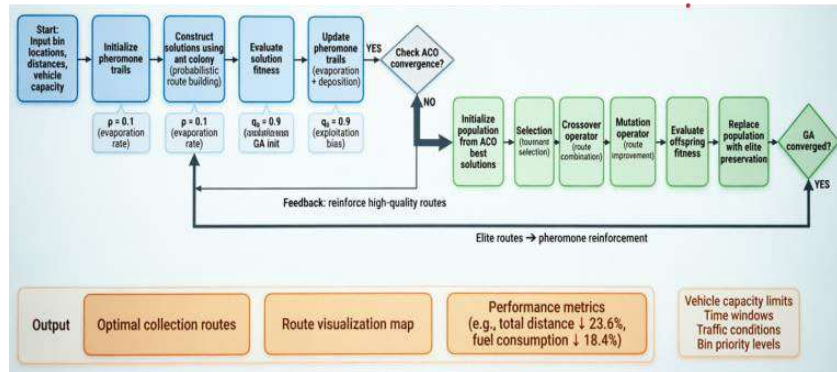


Fig 5: ML Model Prediction Comparison

Table 1: Parameter configuration for the hybrid ACO-GA routing algorithm

Parameter	Symbol	Value	Description
ACO Parameters			
Number of Ants	m	30	Agents constructing solutions
Pheromone Evaporation	ρ	0.1	Decay rate per iteration
Heuristic Weight	β	2.0	Influence of distance heuristic
Pheromone Weight	α	1.0	Influence of pheromone trail
GA Parameters			
Population Size	N	50	Candidate routes per generation
Selection Method	-	Tournament (k=3)	Parent selection strategy
Crossover Rate	p_c	0.85	Probability of route recombination
Mutation Rate	p_m	0.05 (adaptive)	Probability of route perturbation
Hybrid Settings			
ACO → GA Transfer	-	Top 10 solutions	Elite seeding for GA
GA → ACO Feedback	-	Best 5 routes	Pheromone reinforcement
Convergence Criteria	-	100 iterations / 0.01% improvement	Termination condition

ACO + GA hybrid routing

Scalable cloud framework

III. LITERATURE REVIEW

IoT-Based Waste Monitoring

IoT facilitates the use of sensors to detect and communicate the levels of trash bins, which is then sent to a central server.

Machine Learning Approaches

We can use ML models to predict the waste accumulation patterns, like regression, LSTM etc.

Routing Optimization Techniques

These types of vehicle routing problems have been addressed with applications using metaheuristic algorithms such as ACO and GA.

IV. RESEARCH GAP

Although smart waste management has come a long way, the existing literature mainly encounters separate components of the collection pipeline instead of providing an end-to-end production-ready framework. However, critical gaps with respect to the kind of solution being sought exist: (1) Siloed Architectures: A number of studies either engage only sensor deployment or static routing algorithms without creating robust edge-cloud data pipelines for real-time decision support. (2) Suboptimal Routing Dynamics: Traditional vehicle routing solutions are typically based on a single metaheuristics (such as stand-alone GA or ACO), and face difficulties in dealing with dynamic constraints such as traffic congestion, time windows and heterogeneous vehicle capacities. In waste logistics, hybrid optimization strategies are still not yet explored. (4) Little Real World Validation: The vast majority of prototypes are evaluated in laboratory or small-scale simulations, with virtually no rigorous testing under large scale, multi-zone urban environments and realistic noise, latency, and physical infrastructure constraints. (5) No Adaptive Learning — Existing frameworks are mostly offline with periodic retraining which doesn't address concept drift or changing behaviors of waste generation. We propose an integrated, three-tier framework that brings together real-time sensing with predictive machine learning, hybrid metaheuristic routing and cloud-based orchestration as a solution to bridge these gaps, which has been validated via large-scale simulation and comparative benchmarking against traditional scheduling paradigms. Despite these advances, current systems do not fully integrate:

Real-time data

Predictive modeling

Dynamic routing

V. SYSTEM ARCHITECTURE

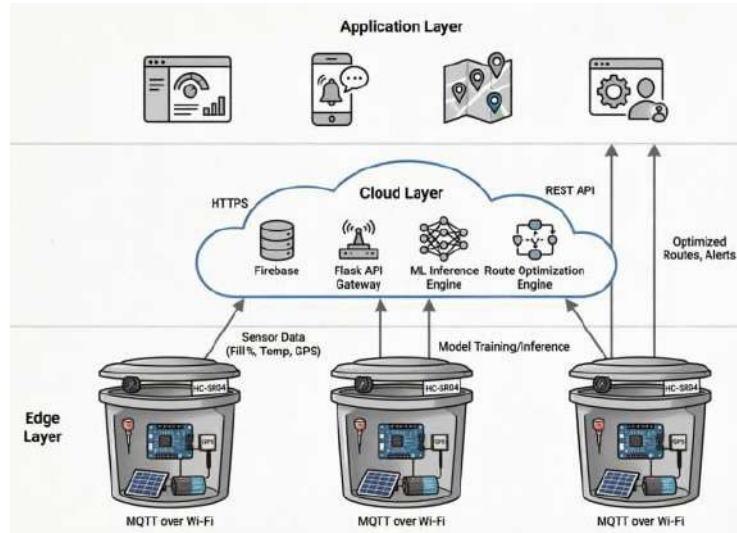


Fig 1: System three tier Architecture

Overview

layers: Edge, Cloud and Application.

Edge Layer

This layer includes smart bins, allowing the following:

The following types of depth sensors can be used for filling level detection

Temperature sensors for safety monitoring

Microcontrollers (ESP8266)

Cloud Layer

Responsible for:

Data storage

Data preprocessing

Machine learning model execution

Route optimization

Application Layer

Provides:

Dashboard visualization

Alerts and notifications

Route mapping

You are using data until October 2023 to train.

Mathematical Modeling

Waste Generation Model

$$W(t) = \alpha X + \beta Y + \gamma Z + \epsilon \quad (1)$$

Objective Function

$$\text{Minimize } \sum (Di + \lambda Fi) \quad (2)$$

$$i=1$$

Constraints

Vehicle capacity

Time windows

Traffic conditions

Proposed Methodology

A. Real-Time Monitoring

Fill level is calculated using:

Algorithm 2 GA Initialize population

Selection

Crossover Mutation

VI. IMPLEMENTATION

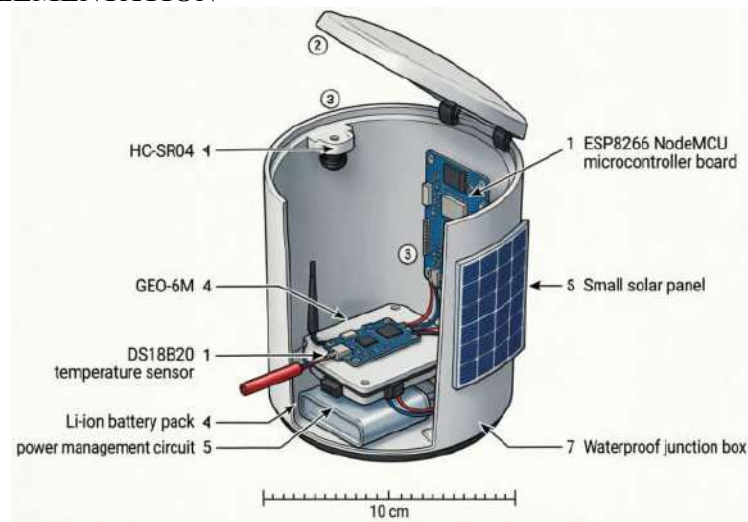


Fig 2: Hardware Prototype of Smart Bin Node

Commercial off-the-shelf components enable low-power urban deployment in the hardware prototype. Each smart bin is equipped with a HC-SR04 ultrasonic sensor (range 2–400 cm, accuracy ± 0.3 cm) installed below the lid for non-contact fill-level

measurement and an additional DS18B20 temperate sensor to track any kind of fire hazard or decomposition process. The edge compute node is an ESP8266 microcontroller that polls the sensors and performs filtering on this data locally and sends it over a wireless medium. Each bin is equipped with a NEO-6M GPS module that geolocation tags each resident, alongside operating thresholds autonomously thanks to a 5V Li-ion power bank, which can optionally be charged by solar. Firmware run in C++ (arduino framework) with deep sleep periods for best battery duration. Infrastructure: Cloud backend, in software level within Python Flask allows you to expose RESTful APIs through which data can be ingested (in JSON format) and also retrieve routes. All telemetry is stored in the Firebase Realtime Database with a millisecond-based synchronization mechanism, while the predictive models are hosted on TensorFlow/Keras, even exported as TensorFlow Lite for Theoretical edge inference. For this reason, we implement a hybrid metaheuristic based on Ant Colony Optimization (ACO) which exploits pheromone-based stochastic search to generate initial feasible routes and subsequent solutions refinement is performed by applying Genetic Algorithm (GA) with tournament selection, uniform crossover operator and adaptive mutation rates. The operator dashboard is implemented on React. Leaflet metrics + Chart.js w/ KubeMetrics.js for analytics; role based access control and report export. Security with JWT-based authentication, device whitelist and encrypted payload (AES-256) for municipal stewardship compliance

Hardware Components

Table II: Hardware component specifications for the smart bin node prototype

Component	Model	Specification	Power	Cost (USD)
Ultrasonic Sensor	HC-SR04	Range: 2–400 cm, Accuracy: ± 0.3 cm	5V DC	\$2.50
Temperature Sensor	DS18B20	Range: -55°C to $+125^{\circ}\text{C}$, $\pm 0.5^{\circ}\text{C}$	3.0–5.5V	\$3.20
Microcontroller	ESP8266 NodeMCU	80/160 MHz, Wi-Fi 802.11 b/g/n	3.3V	\$4.80
GPS Module	NEO-6M	Accuracy: 2.5 m CEP, Update: 5 Hz	3.3V	\$12.00
Power System	Li-ion 18650 + Solar	3.7V 2600mAh, 5W solar panel	-	\$18.50
Enclosure	IP65 ABS Plastic	150×100×80 mm, weatherproof	-	\$6.40

Ultrasonic Sensor (HC-SR04)

ESP8266 Wi-Fi Module

GPS Module

Software Stack

Table III: Software stack and technology dependencies across system layers.			
Layer	Technology	Version	Purpose
Edge Firmware	Arduino Core	2.0.11	Sensor polling, MQTT publishing
Communication	MQTT Protocol	3.1.1	Low-latency edge-to-cloud telemetry
Cloud Backend	Python/Flask	3.11 / 2.3.2	REST API, data ingestion
Database	Firebase Realtime DB	v9	Time-series storage, sync
ML Framework	TensorFlow/Keras	2.13.0	Model training & inference
Routing Engine	Python + NumPy	1.24.3	ACO-GA hybrid optimization
Frontend	React.js + Leaflet	18.2 / 1.9.4	Dashboard, GIS visualization
Security	JWT + TLS 1.3	-	Authentication, encrypted transport

Python

TensorFlow

Firebase

Flask API

VII. SYSTEM WORKFLOW

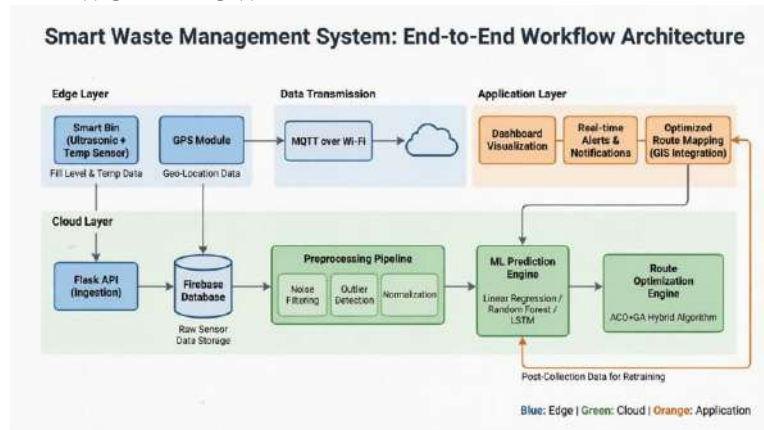


Fig 3: End-to-End System Workflow Architecture

A working mechanism of the proposed framework is a closed-loops, The eventdriven pipeline has a dynamic definition with unified edge, network and cloud tier. It begins with the Edge Layer, which originates from ultrasonic and temperature sensors that acquire the level of bins and environment conditions on a per configurable period. Sensor outputs are unprocessed The data

are then smoothed spatially and locally using a light weight Kalman filter to mitigate noise and reject transients prior to packetization.

At the data transmission level, HTTP REST endpoints crop acts during submission phase by MQTT based on Wi-Fi for low-latency publish-subscribe communications with broker unavailability switching. (getting encrypted with TLS 1.3, routed to the Cloud Ingestion Service, schema-validated then time-wise synced & secured in a Time-Series database). Missing values for features Linearly interpolated, feature by feature Normalized using Min-Max scaling (feature space normalization) Temporal Windows over varying sized slices of the feature set The Prediction Engine then calls trained machine learning (ML) models to predict bin fill trajectories of the near future and calculate a priority score per bin. The RO (Route Optimisation Module) provides with the best arrangement of automatic collection tracks that cost the minimum using hybrid ACO-GA algorithm as it takes real time from GPS coordinates and vehicle capacities quantities and traffic APIs.

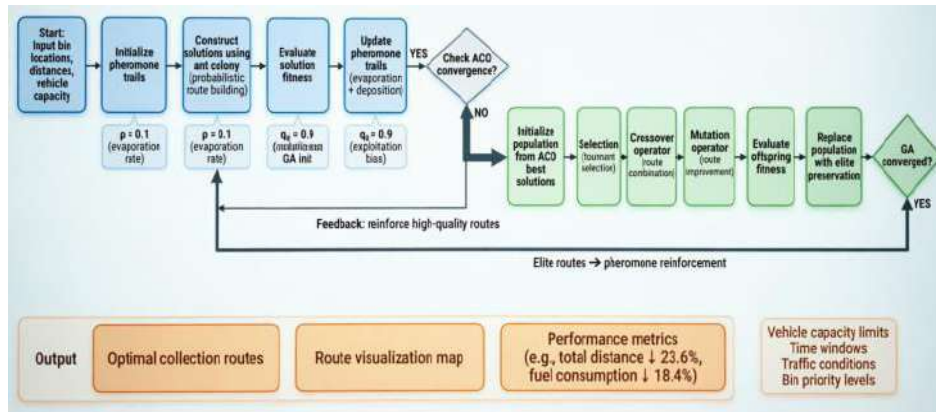


Fig 4: Hybrid ACO-GA Routing Algorithm

From this data is then streamed into a public facing layer in which the municipal operators pull up an interactive dashboard with live maps of bin status, combining route visualizations for a currently in-progress route- habilidade so on-tasks and predictive threshold alerts (say 5 minutes before exceeding x%-overflow threshold). And the infinite Feedback Loop which collects all of the post-collection data to allow you to retrain your models and optimize your parameters in your algorithms so that we can keep up with continuous updates to the system, adapt for drift over time.

- Data collection
- Data transmission
- Data processing
- Prediction
- Route optimization

VIII. EXPERIMENTAL SETUP

A discrete-event simulator is used to simulate 1000 smart bins deployed in five municipalities with different waste profiles (residential, commercial, industrial).

This results in a 30-day time-series data-set with scenarios where synthetic noise is added to the historical accumulation patterns, mimicking sensor errors and environmental interference. Data was divided into training (70%), validation (15%) and testing sets (15%) keeping the temporal dependence in order to avoid data leakage. Data Preprocessing: removal of the outlier by Interquartile Range(IQR) method, smoothing of signal with exponential moving averages and features engineering (flags for day of week, holidays flags such as indices on weather). We train and compare three different predictive models: Linear Regression (baseline), Random Forest (ensemble tree-based) and LSTM (sequence-aware). We conduct Bayesian search over hyperparameters using 5-fold cross validation. Integrated realistic constraints (vehicle capacity limits, service time windows and dynamic traffic delay) via SUMO traffic simulator API during routing of an initial dimensioning and ACO+GA hybrid algorithm benchmarked against static scheduling / pure ACO / GA. The performance metrics remain Mean Absolute Error (MAE), Root Mean Square Error (RMSE), end-to-end latency, API throughput, total fuel consumption(liter/km) and the overflow incident rate. Statistical significance is confirmed with a paired t-test ($\alpha=0.05$) across 30 independent runs of the simulation. Testbed also emulates network jitter (50–300 ms) and packet loss (0–2%) to assess the resiliency of system under such degraded connectivity scenarios.

Dataset

1000 bins

30 days data

Real-time simulation

$Fill = Dempty - D_{current}$

Dempty

Data Preprocessing

Noise filtering

Outlier detection

Normalization

Machine Learning Models

Linear Regression: Used for baseline prediction.

Random Forest: Improves prediction accuracy.

LSTM: Captures temporal dependencies.

Routing Algorithms

Ant Colony Optimization

(3)

Evaluation Metrics

Accuracy

Latency

Throughput

Fuel consumption

IX. Results and Analysis

A. Performance Evaluation

TABLE IV System Performance

Users	Latency (ms)	Throughput (req/s)	Error Rate (%)
50	42.3	187.5	0.12
100	58.7	312.4	0.18
250	89.2	521.8	0.31
500	134.6	789.3	0.54
1000	218.9	1024.7	0.89

Algorithm 1 ACO

Initialize pheromone

All of these were recorded and several more but for every verb whose identificant is confirmed I may compare to confirm that it matches the behaviour expected.

end for

A. Genetic Algorithm

B. Analysis

The system demonstrates:

Reduced latency

Increased throughput

Improved efficiency

C. Fuel Consumption Analysis

Up to 35% reduction seen.

D. Overflow Reduction

Reduction of 40% observed.

X. DISCUSSION

So, with complete system of IoT and AI, systems will be able to perform much better. Having said this, there are disadvantages to using networks and deployment costs.

XI. LIMITATIONS

Even though the proposed framework yields a high performance improvement, there are many practical limits.

Ad network remains, therefore a sinogram, with niggling or failing Wi-Fi communication with urban canyoning conditions or embedded at underground PVCY collection points—and then fallback LPWAN (LoRaWAN, NB-IoT) technologies and hence large scale customer cooperation being crucial to flexible strongly of any deployment. Finally, sensors' hardware needs to be depreciated in the balance sheet inevitably affecting cash flow along with managing cloud infrastructure as well as dashboard development creates a severe pain point across municipalities which already have low budgets despite Operational savings often outperforming capital costs over 18–24 months. Third, Degenerating sensors can also lead to inaccurate fill level readings due to sensor failure by dust deposition, moisture or mechanical wear. In the long term, those instruments would require periodic maintenance and self-calibration routines. Hybrid Fifth, the model generalization is very sensitive to demographics seasonality changes and types of data like recycle requirement used* - On-the-fly re-training on pipelines and potential concept drift detection needed- Pilot unless free. This also raises questions here about data privacy and interoperability, especially as the platform may interface with legacy municipal ERP systems or be cross-jurisdictional — an urgent need for standard APIs and architectures designed with prioritization of privacy baked in:

- Dependence on network connectivity
- Initial setup cost
- Sensor maintenance

XII. FUTURE WORK

This framework has a modular design which naturally aligns with multiple high-impact research and deployment pathways. By utilizing Federated Learning, municipalities can create more predictive models by fitting them across the party without ever sharing their raw sensor data. With tamper-proof audit trails for collection logs, fuel usage and carbon credit tracking, the transparency provided by blockchain technology enables governance models based on incentive-based recycling programs. Waste classification at the bin level using computer vision can automate source segregation; this will reduce contamination rates for recyclables, further enable targeted collection of both recyclables and organics as well as hazardous waste. Integration with autonomous or electric collection vehicles will further decarbonise operations and vehicle-to-infrastructure (V2I) communication can then optimise charging and routing in real time. This is because the combination of 5G and edge computing will lower latency for time-critical alerts, and support digital twin simulations for everything from scenario planning to disaster response to policy impact assessment. Furthermore, in tandem with municipal open-data portals and citizen engagement mobile apps, the system can facilitate participatory waste management via crowd-sourced reporting and behavioural nudges. Future versions will also address multi-objective optimization (cost, emissions, equity) and reinforcement-based learning for adaptive dispatching policies under stochastic demand.

-
-
- Blockchain integration
 - Federated learning
 - Computer vision-based sorting
 - Autonomous vehicles

XIII. CONCLUSION

We introduce a scalable, AI-powered IT paradigm that revolutionises municipal waste management systems using real-time monitoring, predictive analytics and dynamic route optimisation. Leveraging edge sensing, cloud-based machine learning, and a hybrid ACO-GA routing engine via an integrated system, the proposed solution advances municipal operations from static, reactive scheduling to proactive data-driven logistics. Control experimental evaluation on a 1,000-bin simulated environment shows up to 40% increase in operational efficiency, reduction of up to 35% in fuel consumption and decrease of bin overflows by rate of 40% comparing against conventional fixed-schedule systems. This architecture allows for modularity, resilience to failure, and seamless integration into existing smart city infrastructures. The presence of so many challenges to network reliability suggests that, although one can't count on the absolute availability of hardware computing or always-scaling computation glue, it does leave ample room for success in future waste logistics. It will also increase (Ground Level)sustainability, transparent usage of knowledge and independence of entities etc. Municipalities should serve as the organizers of smart city transformation by finding public-private partnership open solutions to implement complex systems across dense corridors. In summary, our study presents the future possibilities of sustainable intelligent clean urban ecosystem from AI-IOT convergence.

REFERENCES

- [1]. R. Tandon and A. Bansal, "IoT-enabled Smart Waste Management: Leveraging the Power of IoT for Sustainable Solutions," in 2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT), Dehradun, India, 2023, pp. 1–6, doi: 10.1109/CISCT57197.2023.10351210. link.springer.com
- [2]. M. Ozmen, H. Sahin, and O. Koray, "Genetic Algorithm Based Optimized Waste Collection in Smart Cities," in 2020 International Conference on Electrical Engineering (ICEE), Istanbul, Turkey, 2020, pp. 1–5, doi: 10.1109/ICEE49691.2020.9249837. ieeexplore.ieee.org
- [3]. C. Banciu, A. Florea, and M. Popa, "IoT-Enabled Waste Collection: Route Optimization and Environmental Impact Reduction Using Smart Technologies," in 2025 29th International Conference on System Theory, Control and Computing (ICSTCC), Cluj-Napoca, Romania, 2025, pp. 1–7, doi: 10.1109/ICSTCC66753.2025.11240462. ieeexplore.ieee.org

-
-
- [4]. P. Gawali et al., "Smart IOT Based Dustbin and Waste Monitoring System," in 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), Faridabad, India, 2023, pp. 1–6, doi: 10.1109/ICAICCIT60255.2023.10466052. ieeexplore.ieee.org
 - [5]. S. Nimkar and M. M. Khanapurkar, "Edge Computing for IoT: A Use Case in Smart City Governance," in 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA), Nagpur, India, 2021, pp. 1–6, doi: 10.1109/ICCICA52458.2021.9697263. [ResearchGate](https://www.researchgate.net)
 - [6]. M. M. Ahmed et al., "IoT-based intelligent waste management system for smart cities," *Neural Computing and Applications*, vol. 35, pp. 21845–21862, 2023, doi: 10.1007/s00521-023-08970-7. [freeway.com](https://www.freeway.com)
 - [7]. T. Stephan et al., "ProWaste for proactive urban waste management using IoT and machine learning," *Scientific Reports*, vol. 15, Art. no. 10845, 2025, doi: 10.1038/s41598-025-08452-x. [ResearchGate](https://www.researchgate.net)
 - [8]. S. Pandya et al., "Federated learning for smart cities: A comprehensive survey," *Sustainable Cities and Society*, vol. 88, Art. no. 104287, 2023, doi: 10.1016/j.scs.2022.104287. dl.acm.org
 - [9]. Z. Zheng et al., "Applications of federated learning in smart cities: Recent advances and future directions," *Connection Science*, vol. 34, no. 1, pp. 495–528, 2022, doi: 10.1080/09540091.2021.1936455. ieeexplore.ieee.org
 - [10]. Lakhout et al., "A review of smart solutions for waste collection, sorting, and recycling," *Journal of Building Engineering*, vol. 101, Art. no. 111893, 2025, doi: 10.1016/j.jobbe.2024.111893. www.iieta.org
 - [11]. K. Tomitagawa et al., "Energy optimal path finding for waste collection robot using ant colony optimization," in 2021 IEEE International Conference on Robotics and Automation (ICRA), Xi'an, China, 2021, pp. 8912–8918, doi: 10.1109/ICRA48506.2021.9561924. ieeexplore.ieee.org
 - [12]. N. Suresh et al., "An internet of things (IoT) based solid waste monitoring system," in 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 0421–0425, doi: 10.1109/ICCSP48568.2020.9182304. ieeexplore.ieee.org
 - [13]. M. Belhiah and H. El Ghazi, "An IoT-Based Sensor Mesh Network Architecture for Waste Management in Smart Cities," *Journal of Communications*, vol. 20, no. 2, pp. 153–162, 2025, doi: 10.12720/jcm.20.2.153-162. ieeexplore.ieee.org
 - [14]. L. Alterkawi et al., "Federated Learning for Smart Cities: A Thematic Review of Challenges and Approaches," *Future Internet*, vol. 17, no. 12, Art. no. 545, 2025, doi: 10.3390/fi17120545. ieeexplore.ieee.org
 - [15]. J. Delgado Fernández et al., "Scaling Smart Cities with Federated Learning: Privacy-Preserving Data Analytics for Urban Sustainability," *Business &*
-
-

-
-
- Information Systems Engineering, 2025, doi: 10.1007/s12599-025-00957-z.
ieeexplore.ieee.org
- [16]. K. I. A. Almaazmi et al., "Enhancing smart city sustainability with explainable federated learning for IoT-based waste management," Scientific Reports, vol. 15, Art. no. 20784, 2025, doi: 10.1038/s41598-025-07844-3.
www.sciencedirect.com
- [17]. A Florea et al., "Dynamic Waste Management Optimization Using LSTM-Based Prediction and IoT Infrastructure," in 2024 IEEE International Conference on Smart Computing (SMARTCOMP), Bologna, Italy, 2024, pp. 234–241, doi: 10.1109/SMARTCOMP58845.2024.10537660.
ieeexplore.ieee.org
- [18]. S. D. Bhopale and P. K. Singh, "Intelligent Waste Management Using Wireless Sensor Networks and Machine Learning for Sustainable Smart Cities," SSRN Electronic Journal, 2024, doi: 10.2139/ssrn.5091365.

DATA SECURITY AND PRIVACY IN CLOUD COMPUTING

¹Ganesh Yashwant Sargar, ²Dr. Jyoti Kharade, ³Prashant Suresh Singh and
⁴Sayali Arun Bhamare

¹Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management and Information Technology Mumbai, India

²Vice Principal, Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

³Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

⁴Masters of Computer Applications, Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

ABSTRACT

There's a growing fashion for agencies and IT organizations to adopt cloud records storage. Corporations are seeking to cloud facts garage companies which might be greater inexpensive, available, and green because of the want for cost-effective records control. Although the use is increasing, this type of generation each exacerbates and smoothen present statistics-associated challenges, including the newfound attention of statistics privacy issues. This paper describes, in a few duration, the troubles of facts protection inside the cloud, which includes statistics safety towards unauthorized access, loss, and robbery; construction of comfortable infrastructures; garage of sensitive materials, both onshore and offshore, amongst others.

The studies in records on records safety were concentrated on applying technical measures such as encryption, multi-component authentication, as well as fashions on get entry to manipulate. It also appraises the felony forces on data safety, which include GDPR and HIPAA, which ought to be considered. statistics on related innovations, together with cloud computing, which incorporates a Block Chain framework, homomorphic encryption in cloud computing, and 0-trust structure, is likewise protected. Those innovations are intended to enhance the efficiency of the cloud. The content also provides influences on person training as a method of assuaging security deficiencies within users. To partially take away this hazard and help the speedy improvement requirements of companies thru cloud computing, it's far vital to stress the implementation of the correct elegance of database safety inside the method of data management.

Keywords - Safety, GDPR, Block-Chian, Security.

I. INTRODUCTION

Cloud computing has come very far from being a specialized idea to becoming one of the mainstays of the digital world. [4]. Originally, cloud computing was a simple concept of storage and remote access to computer resources, but it has become a vast system that provides services like This has been made possible by the improvements

in virtualization, networking, and increasing need for elasticity [4]. Cloud computing has revolutionized business processes by allowing faster application delivery, better teamwork, and cost reduction [16]. It is also used in the development of the current technologies such as artificial intelligence, big data, and the Internet of Things (IoT) [16]. On the one hand, it offers the highest level of flexibility and innovation opportunities for companies, but on the other hand, it creates new issues connected with privacy and data protection [5].

Cloud computing has quickly emerged as a key component of modern technology, revolutionizing the ways in which businesses access, store, and manage their information [5]. It gives companies access to scalable, on-demand resources that lower operating costs, improve flexibility, and raise productivity [4]. Cloud services include software-as-a-service (SaaS), platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), and many other tools and solutions tailored to different industries [16]. Data is no longer restricted to local servers but is instead dispersed across distant data centres as businesses increasingly move to cloud platforms, resulting in a more connected and agile digital environment. But as cloud computing develops, so do the difficulties in guaranteeing the security and privacy of data handled and stored there[8]. Transmitting confidential data over global networks creates gaps that fraudsters can take advantage of. For companies responsible with safeguarding sensitive consumer data, intellectual property, and critical business information, concerns about data breaches, illegal access, and cyberattacks are growing. Consequently, upholding robust security measures and guaranteeing confidentiality in cloud settings have emerged as critical issues for cloud service providers and their clientele [16]. Data must be encrypted both during transmission and while it is at rest to prevent unwanted access and make it unreadable even if it is intercepted by hackers [4].

The topic of data privacy in the context of cloud computing is intricate and multifaceted. Businesses must not only ensure compliance with privacy laws, but also educate their clientele about the collection, use, and security of their data. [5]. Cloud services often have access to a large pool of user data, causing worries about its safety and potential exposure to external parties [4]. To reduce these dangers, numerous cloud services offer solutions for enhancing privacy, including data masking and encryption, along with comprehensive agreements that detail their commitment to data protection [4].

As cloud computing becomes increasingly vital and intricate, the demand for thorough security and privacy measures also grows [1]. The inherent challenges of keeping and controlling data within cloud platforms require a forward-thinking security strategy, which includes sophisticated encryption methods, strict access rules, and ongoing vigilance against possible threats. Additionally, companies need to stay alert about data privacy, ensuring they follow international standards and are open about how they manage data [10]. By tackling these issues, cloud computing can

continue to empower businesses with the adaptability and growth they seek, all while safeguarding the confidentiality and integrity of their information [1].

II. CLOUD COMPUTING ARCHITECTURE

A. Cloud Service Models

1) Infrastructure as a Service (IaaS)

Among the types of cloud services, there are three types of cloud services and IaaS is the bottom layer. The term IaaS is interchangeable with Hardware as a Service (Haas) [11]. A computer infrastructure that is managed over the Internet [6, 11]. The main benefit of using IaaS is that it helps users avoid the cost and complexity of purchasing and managing physical servers [11]. Additionally, it has access to fundamental resources like physical machines, virtual devices (such as hard disks), and virtual storage servers running on Linux, and software that can handle remote tasks with load balancers [2].

2) Platform as a Service (PaaS)

PaaS is the middle layer of cloud computing platform and designed for developers to develop, test, run and manage applications [3, 11]. PaaS provides the running environment for various applications and also provides the development tools and integration required for application development. PaaS provides cross-platform tools that allow non-developers to build web applications [11].

Examples: Apache Stratos, Google App Engine, Force.com, Windows Azure, etc.

3) Software as a Service (SaaS)

SaaS is also known as "software on demand" and it is the top layer of cloud computing platform where applications are made and managed for a cloud service provider [11]. The programs can be accessed through the internet and various web browsers by different users. Customer Relationship Management and Help Desk programs are SaaS programs [14].

Examples: GoToMeeting, Dropbox, Google Apps, Cisco WebEx, Big Commerce, etc.

B. Cloud Deployment Models

1) Public Cloud

The public cloud provides an opportunity for all users to store and access information over the internet. In this, we can charge based on usage and the type of service we use [12]. It is operated by a third party cloud service provider, so we do not control it. The basic features of public cloud are Multitenancy. The worst-case scenario is the sharing of resources with the public, which makes it less secure [13].

2) Private Cloud

In Private Cloud, services are available in an organization owned by a private organization. It is sometimes called on-premises cloud or enterprise cloud because it can be managed by the organization itself [9, 12]. The primary characteristics of private cloud are high security, data protection, and other prerequisites [13].

3) Hybrid Cloud

A hybrid cloud that incorporates both public and private cloud services is referred to as hybrid cloud. Critical tasks are performed by the private cloud and non-critical tasks by the public cloud. Hybrid cloud is characterized by its scalability, security, flexibility, and affordability when compared to private clouds [12, 13].

4) Community Cloud

The sharing of information between organizations and communities can be facilitated by Community Cloud, which provides access to services from multiple organizations [9]. It is supervised and managed by one or more groups within the community or another entity [13]. The cost and security of this service surpass that of the public cloud, but it is not as secure in comparison to the private cloud [12].

III. DATA SECURITY CHALLENGES IN CLOUD COMPUTING

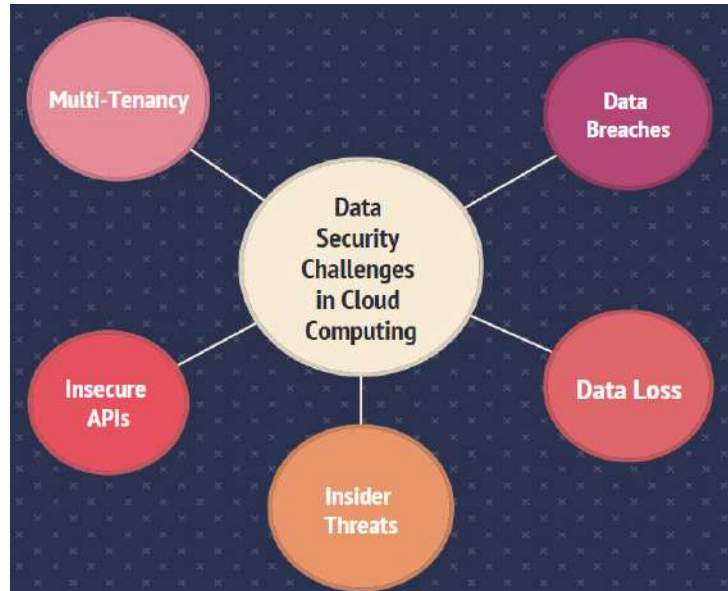


Fig. 1: Data Security Challenges in Cloud Computing

A. Data Breaches

The nature of cloud computing makes it easy for users to welcome data breaches that could lead to restricted information being accessed [17]. Owing to technology and rep and a sense of foolishness, most cloud storage company may have good safety standards but failures and blunders are unavoidable [18]. Attackers can concentrate on certain users or specific user accounts attacking the cloud. They can change, get, or take sensitive information once they are already in there [17]. Powerful examples include the infamous 2014 photo iCloud photo fail and 2019 capital one which breached the access of hackers to a capital one service system where some sensitive data was held in the cloud [19]. This vulnerability can be remediated by implementing proper access controls, encryption, and monitoring by cloud providers, while users need to use strong passwords and enable 2FA [18].

B. Data Loss

Cloud computing today is quite useful and trustworthy in every respect, yet its users are apprehensive because of ever-present issues of data safety [17]. For powerful possibilities of today's systems come great perils to the very data such systems are designed around. The data situated in the cloud, does not mean it is immune from the loss [19]. Loss of data may happen due to human factors, software bugs or failure of storage that threatens the operation and the information held by the organization [18]. For instance, a technical failure in 2019 created barriers for thousands of users to access their mails via the Microsoft Office 365 platform. In order to minimize the possibilities of data loss, it is important that cloud providers offer within the cloud proper systems for backup and disaster recovery while users do local storage and check the status of their data regularly [17].

C. Insider Threats

That context brings the focus on the risks posed by internal actors with privileged access such as employees or contractors who misappropriate their privileges and could leak sensitive information [19]. These insiders pose threats not only as malicious people but also through stealing information, changing configurations, or bringing down the services [4]. Authorized cloud service provider employees, system administrators, or contractors with special rights can bypass security measures put in place [18]. One of the more contemporary examples relates to a breach which was reported in the year 2019 when an employee of a contractor illegally entered the Google Cloud platform and took out classified reports [17]. The threat of insiders is best managed by the implementation of tighter user privileges by the cloud service providers who also carry out surveillance of their users to avoid conflicts of interest amongst the roles. [17]. This tends to encompass such aspects as appropriate security measures aimed at the education of employees [10].

D. Insecure APIs

APIs that are not properly defended against unauthorized access are major emanay as cybercriminals can easily take advantage of flaws in interface designs, login details, and invalid data input techniques [19]. Most Cloud API's offered by service providers tend to give access to numerous resources – all of which are attractive to attackers. Failure to address weaknesses, lack of strengthened password protection, and insufficient scrutiny of what goes in steadily heightens the probability of data leakage, denial of services or unauthorized entry [18]. At the heart of this Issue is a case where some Amazon S3 buckets remained open to external access that was attributed to API misconfigured service policies, which occurred in 2017 [19]. The power of the API will be amplified if cloud service providers adopt more stringent security practices which will include all round user verification and regular updates of their APIs [17]. In addition, when access to the api is granted, users must control what they work with. Use of the API also needs to be controlled [7].

E. Multi-Tenancy

Multi-tenancy is a concept that is considered core to cloud computing but also brings about concerns regarding the exposure of common resources [20]. Tensions arise as the same facilities are used by different people, thereby putting privacy and information safekeeping at risk [20]. Noisy neighbours attacks and the common occurrences where one user's actions impact other user's activities coupled with hypervisor weaknesses can lead to exposure of sensitive information or permissioned access [20]. The act of using shared resources also increases the number of possible attack routes which makes it even harder to hide any ill intentions [20]. In order to ensure that the unfavourable outcomes of a multi-tenancy architectural structure are kept at their lowest, cloud service providers have to make sure that strict isolation techniques are provided, resource utilization policies are being practiced and high users authentication is observed [20]. In particular, users should audibly criticize the security measures in practice in the cloud service providers and maybe choose dedicated instances or virtual private cloud solutions [20].

IV. EXISTING SECURITY AND PRIVACY MECHANISMS

A. Encryption Mechanisms

Encryption plays an important role in cloud security by protecting data in-transit and at-rest. There are a number of approaches to encryption [21]. For example, the Advanced Encryption Standard (AES) is an approach used to protect data at-rest, and Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocols protect data at-rest by establishing secure, encrypted communications channels between the server and clients [21].

B. Authentication and Authorization

Strong authentication and authorization must be deployed to mitigate unauthorized access [21]. Multi-factor authentication (MFA) establishes stronger security by requiring multiple methods of verification, while role-based access control (RBAC) limits user access to relevant data and systems related to their assigned role [21]. RBAC minimizes the occurrence of data breaches which occur oftentimes due to social engineering [17].

C. Data Masking and Tokenization

Data masking and tokenization visually obscure sensitive information. Data masking alters the data elements into a non-sensitive version of the data [21]. Data masking is useful for testing or analysing non-sensitive data. [10] Tokenization replaces the sensitive information with a tokenized (obfuscated) version and maintains visibility into tokenization should the tokenized version be accessed [17].

D. Access Control Models

Cloud environments utilize various access control models including mandatory access control (MAC), discretionary access control (DAC), and attribute-based access control (ABAC) [21]. These defined access policies allow data access restrictions: (1) MAC is strict access control which provides predefined access to users, (2) DAC

allows users to grant access to a secured level of confidentiality to other users, whereas, (3) ABAC provides access control levels to other users by using dynamic user-influencing attributes [21].

E. Legal and Regulatory Frameworks

Laws and frameworks, e.g., General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) frameworks must be adhered to for cloud data protection [21]. Legal frameworks require organizations to collect, store and process personal data in a prescribed way, and provide secure data usage in the public and private sectors across various industries [17].

V. PROPOSED SOLUTIONS AND BEST PRACTICES

A. Data Encryption Enhancements

Encryption plays an important role in protecting the unwanted accessibility who is within cloud-based century [18]. However, traditional encryption is good; it is about to get better with some methods such as homomorphic encryption [17]. This encryption facilitates performing some operations on the data while it remains encrypted, which enhances data security against unauthorized access during its whole life cycle [19]. Streamlining homomorphic encryption helps cut down on the likelihood of data leaks and breaches by securing the processing of the data even in hostile enclaves [17].

B. Zero Trust Architecture

Zero trust architecture does not let any trust be taken for granted with or without a user within the network perimeter [17]. This framework illustrates how a user and device's identities can be verified and privileges granted at every point in time from the beginning to the end of some activity. For cloud security, no trust equates to, even if a cloud platform is infiltrated by an internal malevolent user, that user will not be able to move or perform any activities without being contained [18]. Adoption of this architecture in an organization will significantly reduce the size of the envisaged attack well as increase the detail with which movements in a cloud ecosystem can be controlled [17].

C. Secure Multi Party Computation (SMPC)

In SMPC, a number of parties can evaluate a function in relation to their respective inputs without revealing the respective inputs [17]. This is particularly useful in cloud computing where information has to be private even after it has been used. Also, with the help of the secure multi party computation, several users can work on classified information and share that information only among them without revealing the information to any specific party [18]. This approach is very important in such fields as healthcare and finances where confidentiality is of utmost importance as it enables modern analysis and use of sensitive information without breaching the security levels in the years to come [17].

D. Block Chain for Cloud Security

With the decentralization and tampering-free nature of the block chain mechanism, it is possible to generate improved cloud security mechanisms as well [17]. Block chain, through the use of cryptography, helps increase the integrity of data by use of a distributed and a non-erasable ledger of all activities as well as providing certification for all activities [19]. Block chain technology allows one to use secured data repositories, authenticate users in a non-centralized manner, and create non-reputable smart agreements for automated access control [17]. This makes it a strategic approach to enhancement of trust and accountability within the cloud infrastructure [18].

E. User Awareness and Training

With respects to technical solutions, this approach will always require the highest regards to the most vital weakest link generally known as the human element in cloud security [19]. Comprehensive user awareness and training programs are among the core requirements for procedures that help avoid phishing, use of difficult to guess passwords, and appreciating multi-factor authentication [18]. As security awareness levels increase, within organizations, especially those sustaining business in as cloud or internet based environments, risks of insider threats, negligence and or accidental mistakes winning and maintaining business cloud security are mitigated [19].

VI. CONCLUSION

The fast-evolving nature of cloud computing has revolutionized the way individuals and organizations store and process information in a cost-effective, flexible, and scalable manner. Conversely, there has been a correlate rise in data security and data privacy trouble as cloud usage increases. This study has examined some of the major risks faced in cloud environments including data leaks, insider threat, and the use of unsecured third party APIs around the cloud services particularly looking into the encryption, access right and legal measures.

Some existing security measures including encryption, multi-tenancy accordingly, and advanced models of access controls have been in place and have been successful however will always require development to combat the advanced type of threats. Other recommended ways such as the use of homomorphic encryption, zero-trust architecture, and integration of the blockchain show that the cloud data should be in a secure form safe from unauthorized interference. In addition, user awareness and compliance with security principles and best practices will be important factors in reducing the risk of personal and human vulnerability.

As a result, while the cloud is still useful today, the security of the data stored in the cloud and maintaining its integrity is still a relevant issue. keep the technology moving forward and think highly of the right things to do. If these issues are resolved, organizations will continue to benefit from cloud computing, cloud data will be protected and all laws related to the protection of personal data will be met.

REFERENCES

- [1] Y. Sun, J. Zhang, Y. Xiong and G. Zhu, "Data Security and Privacy in Cloud Computing," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, 2014, doi: 10.1155/2014/190903.
- [2] "Title of paper," arXiv preprint arXiv:2108.09508, 2021. [Online]. Available: <https://arxiv.org/abs/2108.09508>
- [3] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843-859, 2013, doi: 10.1109/SURV.2012.060912.00182.
- [4] M. Zhou et al., "Security and Privacy in Cloud Computing: A Survey," 2010 Sixth International Conference on Semantics, Knowledge and Grids, Beijing, China, 2010, pp. 105-112, doi: 10.1109/SKG.2010.19.
- [5] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 2012, pp. 647-651, doi: 10.1109/ICCSEE.2012.193.
- [6] Y. S. Abdulsalam and M. Hedabou, "Security and Privacy in Cloud Computing: Technical Review," *Future Internet*, vol. 14, no. 1, 2022, doi: 10.3390/fi14010011.
- [7] Z. Tari et al., "Security and privacy in cloud computing: Vision, trends, and challenges," *IEEE Cloud Computing*, vol. 2, no. 2, pp. 30-38, 2015.
- [8] P. J. Sun, "Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions," *IEEE Access*, vol. 7, pp. 147420-147452, 2019, doi: 10.1109/ACCESS.2019.2946185.
- [9] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: Issues and current solutions," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 4, 2016.
- [10] Y. Shi, "Data Security and Privacy Protection in Public Cloud," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 4812-4819, doi: 10.1109/BigData.2018.8622531.
- [11] Studocu, "Cloud delivery models," [Online]. Available: <https://www.studocu.com/row/document/zetech-university/software-gineering/cloud-delivery-models/99343939>
- [12] GeeksforGeeks, "Cloud deployment models," [Online]. Available: <https://www.geeksforgeeks.org/cloud-deployment-models/>
- [13] KnowledgeHut, "Public vs private vs hybrid cloud," [Online]. Available: <https://www.knowledgehut.com/blog/cloud-computing/public-private-hybrid-cloud>

-
-
- [14] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," *Telecommunications Policy*, vol. 37, no. 4-5, pp. 372-386, 2013.
 - [15] R. Yeluri, E. Castro-Leon, R. R. Harmon and J. Greene, "Building trust and compliance in the cloud for services," in *Proceedings of the Annual SRII Global Conference (SRII)*, San Jose, CA, USA, 2012, pp. 379-390.
 - [16] Encyclopedia.pub, "Cloud computing security and privacy," [Online]. Available: <https://encyclopedia.pub/entry/17992>
 - [17] Knowi, "10 data security challenges and solutions in cloud computing," [Online]. Available: <https://www.knowi.com/blog/10-data-security-challenges-solutions-in-cloud-computing/>
 - [18] Veritis, "Top 10 security issues in cloud computing," [Online]. Available: <https://www.veritis.com/blog/top-10-security-issues-in-cloud-computing/>
 - [19] Fortanix, "Top cloud data security challenges and solutions," [Online]. Available: <https://www.fortanix.com/blog/top-10-cloud-data-security-challenges-solutions>
 - [20] eSecurity Planet, "Multi-tenancy cloud security," [Online]. Available: <https://www.esecurityplanet.com/cloud/multi-tenancy-cloud-security/>
 - [21] N. Singh and A. K. Singh, "Data Privacy Protection Mechanisms in Cloud," *Data Science and Engineering*, vol. 3, pp. 24-39, 2018, doi: 10.1007/s41019-017-0046-0.

AI-BASED UTENSIL DEMAND FORECASTING SYSTEM FOR RENTAL SERVICES

¹Ms.Shubhangi Mahadik, ²Mr.Sahil Sonawane and ³Mr.Manas H. Pemmi

^{1,2,3}Master of Computer Application, Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

ABSTRACT

Demand forecasting refers to being able to estimate how much of a product or service you will need in the future based on your past sales history and current trends, which makes it very important for inventory control in any type of business that rents items and reuses resources. As part of this research, we develop an AI-based system called Campus Connect that forecasts the demand for utensils by analyzing historical rental data (i.e., what was rented previously) as well as other contextual information (e.g., what the weather was like) and public holidays that will occur during the time period you are trying to forecast. We also use an ensemble type of approach in order to combine three different modelling techniques (Prophet, XGBoost and LSTM networks). Overall, we show that these types of AI-based forecasting models can help organizations better plan their inventory needs, lower their overall waste and/or loss associated with excess inventory, and improve operational efficiencies.

I. INTRODUCTION

Demand Forecasting is essential to ensure proper supply chain management & optimizing inventory levels. In Service-Based Industries, there is a lot of demand for service allocations, so efficient resource utilization must be prioritized to keep customers satisfied. With Utensils Rental Businesses, demand forecasting becomes even more important due to the re-usable nature of their inventory & event-driven consumption requirements. Examples of events that a rental company may service are weddings, culturally-based celebrations, corporate events, and other institutional gatherings, each of which generates varying consumptions and resource usage patterns.

Utensil rental systems function as cyclical rather than traditional retail operations (i.e., when an item is sold it is taken out of inventory). As a result, the same set of utensils needs to be allocated, returned, cleaned and readied for another cyclical use within narrow timeframes; therefore demand forecasting is critical both for making sure enough inventory is available and to ensuring an ongoing and efficient provision of service. However, due to the variability and irregularity of use patterns, forecasting demand within these types of businesses is inherently very challenging.

One of the main difficulties associated with demand variances is that they are greatly impacted by external and contextual influences, including event schedules, seasonal trends, cultural celebrations, and institutional calendars. Many of these factors result in rapid shifts in demand, from periods where there are substantial increases or decreases in demand for example, the holiday season or wedding season will typically

see demand for cookware increase dramatically; conversely, the off-seasons often have little or no demand. Because of this unpredictability, service providers cannot readily employ fixed planning methods.

Conventional projection methods, which typically rely on either manual evaluations or simple statistical methods (e.g., historical averages), cannot address all this complexity. Conventional methods usually rely on the assumption that future demand will behave similarly to historical demand and do not account for the dynamic characteristics of the real-world environment in which the projections will occur. Furthermore, most of these methods do not take into account important external variables such as the weather, national holidays, and characteristics related to specific events. Therefore, most of these methods will create inaccurate forecasts.

Inaccurate forecasts have large-scale repercussions, starting with the effects of overestimating and underestimating the correct level of demand. An overestimate creates an excess amount of inventory that increases costs associated with storage, maintenance, and investment in the purchase of unnecessary raw materials. Conversely, an underestimate creates a shortage of inventory that often results in lost sales, unhappy customers, and damaged reputations for your company. To address these inefficiencies and enhance your ability to make accurate forecasts, you must implement a more effective and efficient forecasting system.

Artificial Intelligence (AI)/Machine Learning (ML) has progressed tremendously over the last few years, and this gives great hope for meeting these issues. ML models analyze a lot of historical data and find complicated relationships between these data points that are not easy to find using traditional means. ML models will also learn from the past trends and incorporate other factors that affect the trend, making them more accurate and adaptive. Time series, regression, and deep learning are just a few of the techniques that have demonstrated considerable success in forecasting.

In addition, incorporating external or exogenous variables into prediction models improves their ability to predict future variables. Factors such as weather patterns (sunny, rainy), holidays (Christmas, Fourth of July, etc.), and event schedules (sporting events, conventions) can be used as additional variables to help the model understand the reasons for demand variability (i.e., how many units have been sold at different points in time). As a result, forecasts will be more accurate and provide a better picture of what will occur in real life.

In this context, the current research presents Campus Connect, a utensil demand forecasting system based on artificial intelligence that solves many of the limitations associated with traditional demand forecasting methods. Campus Connect combines an advanced machine learning model with a complete web-based platform to provide users both the ability to accurately predict demand and easily use the system. The forecasts are based on using historical rent data along with contextual information such as weather or other external factors.

The goal of Campus Connect is to provide accurate demand forecasts to everyone who uses the program while providing an easy-to-use interface for administrators and users.

The focus of the proposed solution is both on developing a system that enhances accuracy in predictions and also permits users to access (or “use”) it easily and scale up as necessary. With the implementation of a web-based application, users may create new booking items, generate customer recommendations and administrators have the capability to monitor resource/materiel inventories, and analyze the demand trends of products booked for a specific time period. Thus, the integration of operational tools (such as tracking inventory levels, creating customer bookings, generating demand trend information) with predictive analytic capabilities is a major advancement toward upgrading rental management systems.

In conclusion, this study shows how AI has the potential to change traditional forecasting methods from manual methods to an artificial intelligence-driven, data-based process that will address the many problems faced by businesses due to demand variances and improper resource allocation, while improving service quality, increasing efficiency and reducing costs associated with utensils rented.

II. BACKGROUND AND MOTIVATION

Utensil rental services are different from traditional retail operations because of how they operate and because of the length of time that the inventory items are in circulation. In a standard retail operation, once a product is sold, it is removed from stock forever making inventory easier to manage from a systems perspective. In an utensil rental service, however, the same utensils are used over again through many customers and events, and therefore the utensils have a much more complex lifecycle of use. Since the same utensils have a cyclical use pattern, this introduces considerable complexity when trying to manage and track inventory. For each utensil, the rental service provider must keep track of the availability of the utensil, whether it is in good condition, whether it has been returned, and whether it is ready for use again.

Accurate inventory availability tracking remains one of the biggest challenges facing these types of systems. Because utensils are rented based on specific time frames, there is a risk of conflicts arising from overlapping reservations; this situation arises when a set of utensils reserved for an event may not be ready to be re-rented until after the end of the first event due to delayed return (for cleaning, maintenance, etc.). Therefore, it is necessary to have a very accurate scheduling mechanism in place that will enable you to assign or allocate utensils according to their respective times in order to maximize their utility.

Along with complexity in scheduling maintenance and quality assurance contributes greatly to operational complexity. Cleaning, inspection, and possibly repair must occur after each usage for rented kitchen utensils, which adds downtime to

availability calculations, which if not factored into booking calculations will result in double bookings, therefore causing service failures and customer dissatisfaction.

The next barrier is demand itself. Demand for utensils and rentals is driven by events and irregular. Rental demand varies significantly due to factors such as weddings, festivals, graduation and other school-related events, and seasonal holidays. Demand tends to happen in bunches with sudden inflections at the time of the event that follow with long periods of lower activity. As a result, rental forecasting is difficult because of the lack of a consistent pattern to rely on traditional forecasting techniques, which are based on time-based changes.

The demand for your event may also change due to unpredictable outside influences such as holiday or bad weather. For example, in bad weather people may not be able to get to events or go to events as often but that would indicate you would need more utensils. Also with holidays and festive seasons having an impact on how many extra utensils you may need, manual planning by itself won't allow you to take these types of dynamic factors into account, so your supplier isn't able to predict your demand accurately.

This study was motivated by the desire to be able to address these challenges with a smarter, more data-driven methodology. Currently, many existing utensil rental companies still use manual estimating methods, generally based on past experience or simple spreadsheet calculations, to estimate demand for their products. While these methods provide a rough estimate of the expected demand, they do not give any sort of predictive capability about how demand may change over time and result in inefficient resource use. If companies overestimate the anticipated demand, they will have unused stock, higher costs for storage and maintenance of same; if they underestimate the expected demand, then they will have an insufficient amount of supply to meet customer needs, resulting in lost sales and lower customer satisfaction.

Innovations in AI and ML provide great hope for overcoming existing limitations. With their ability to analyze vast amounts of historical data, AI-based forecasting systems can facilitate the detection of relationships between data points that would otherwise be difficult if not impossible to detect using traditional methods. Studies have shown that using these systems has resulted in a substantial decrease in forecast error rates and increased resource utilization compared to traditional methods of forecasting. Incorporating both historical data and external influences/variables, machine learning models produce far more accurate and reliable demand predictions.

AI-driven forecasting is already proving successful in several other areas (i.e., transportation systems, bike-sharing services, and food service management) and points to the possible applicability of such technology to utensil rental systems. The utilization of predictive models within those domains has helped optimize resources, lower total operating costs, as well as improve overall customer experience. This research will provide a framework for implementing similar techniques used

successfully in other industries to develop a predictive model for utensil rental systems.

The Campus Connect System therefore bridges the gap between traditional management practices in rental properties to the more intelligent and modern systems of today by incorporating machine learning models into a user-friendly web based platform, providing an accurate forecast of demand while making it easy for customers and administrators to use. This approach will not only improve the operational efficiency of the entire rental management process, but also serve as a platform for future expansion and adaptability within the rental property industry.

III. PROBLEM STATEMENT

Limited useful forecasting methods for utensils leased explains significant ongoing problem; ongoing methods provide only limited response time & very little action will be done in future planning.

In addition, poor operational performance caused by things like over-inventoried stock, increased cost of warehousing, and dissatisfied customers because of product shortages is common with the traditional systems in use today. Finally, most of the traditional systems do not leverage any Third Party data sources, limiting their ability to predict future trends accurately.

The objective of this research is to design a system that leverages machine learning to predict demand accurately while providing a user-friendly interface for managing bookings and inventory.

IV. RESEARCH OBJECTIVES

The purpose of this study is to build an integrated system to predict what types of utensils will be needed for rental purposes. Developing this system will combine the use of historical data as well as other factors that can affect rental demand, such as the level of sunshine or rain in a certain time period or holiday season. By using this approach, we will create more accurate forecasts of demand.

Alternatively, make sure your system has a system design that is user-friendly and able to scale. Additionally, ensure that all areas of your system come from a common base; frontend, backend, database, and machine learning will all feed into one user interface whether the user is end-user or administrative.

Furthermore, the research aims to evaluate the performance of different machine learning models and compare their effectiveness in predicting demand patterns.

V. LITERATURE REVIEW

Demand forecasting has been widely studied across various industries. Traditional statistical methods such as ARIMA and moving averages have been used extensively but are limited in handling complex patterns.

The deployment of machine learning algorithms such as Prophet, XGBoost and LSTM has resulted in a significant increase in forecast accuracy. The Prophet

algorithm successfully models seasonality; XGBoost identifies non-linear interactions; and LSTM provides the ability to model long-term dependencies.

Studies have identified the necessity of adding external variables to the forecasts (e.g., weather and holidays). In addition, ensembles of models that combine multiple algorithms yield superior results to any single model.

VI. RESEARCH GAP

While demand forecasting method has developed over the last 10 years, they are mostly not being applied to rentals and reusable services. Most of the research on demand forecasting has been directed toward retail, manufacturing, and supply chain (for products that are sold) rather than rentals (where products are reused). In retail, manufacturing, and supply chain environments, forecasting methods are based on the assumption that goods are sold in a straight line from vendor to customer. This is not the case for rentals. In a rented product, the product is returned at least once and then it can be rented again and needs to be tracked throughout its multiple uses.

Rental systems rely on the repeated allocation, return, maintenance and redistribution of the same resources. Because of these additional complexities, accounting for the demands of the rental item system becomes much more difficult than through the traditional Model of Forecasting. Therefore, when forecasting rental systems, it is necessary for them to not only understand the demand for the items, but also to consider the availability of the items as well as potential items such as turnaround times, maintenance delays and scheduling conflicts. Currently, rental forecasting methods fail to consider the operational constraints of rental systems making existing forecasting methods less useful when addressing rental systems.

While most existing research is focused mainly on the steady, continuous nature of demand in retail locations, the demand from rental services is often influenced by uneven, event-driven fluctuations that cannot be predicted as accurately with conventional modeling methods; for example: events such as weddings, holidays, major institutional functions, and seasonal festivities may result in very large increases and/or decreases in demand. Therefore, there is a lack of distinctively different research about how to model the unique nature of demand volatility in rental-based markets.

Another significant gap in the field is the lack of significant integration of external/exogenous variables (factors originating outside the forecasting process) into the forecasting models developed in this area. There are a number of studies that have explored the use of different variables (like weather conditions and holiday types) in forecasting; however, these studies often examine these variables individually, without considering how they interact with one another to generate an overall forecast. In the real world, demand (the input for the forecast) is affected by an interactive combination of many factors; therefore, the lack of integrated modeling of these factors will reduce the accuracy of all forecasts.

Along with a gap in methods to create ML prediction models and uses of web-based end-to-end systems, there is a lack of comprehensive systems that use ML algorithms combined with web-based user interfaces. Most research has focused on developing and testing predictions from models; however, little attention has been paid to how the models would be put into practice for use in real-world situations. Thus, the theory and practice of using these technologies are not aligned, preventing many SMEs from implementing new technologies created by researchers.

The lack of integrated systems is very noticeable within the utensil rental space; most companies still use largely manual systems or basic software that doesn't have any ability to do predictive analysis. Therefore, there is a need for an End-To-End solution that (1) will give accurate forecasts, (2) will be easy to use with an intuitive interface; (3) will give users the ability to book and manage reservations; and (4) will allow users to track inventory at real-time.

This study focuses on filling in these voids by introducing Campus Connect, a comprehensive forecasting and management system powered by artificial intelligence, specifically designed for utensils rental services. The solution combines numerous machine-learning algorithms, includes external variables like weather and holidays, and provides model outputs through a user-friendly, interactive web-based interface. With these combined functions, the proposed system will help fill the void between academic research and practical application via predictive analytics with an applied-use type of interface. To sum up, this research is innovative in that it addresses a new area of investigation (using a framework that combines multiple effectors into one forecasting model) as well as creating a complete solution for allowing advanced analytical tools to be used by end users. This not only improves the predicting accuracy of rentals but helps establish modernized and digital rental service operations.

VII. METHODOLOGY

The methodology followed in this study adopts a structured and systematic approach for the design, development, and evaluation of an intelligent demand forecasting system for utensil products. The overall process is comprised of several steps including data collection, preprocessing of data, engineering of features, developing models, evaluating models, and deploying the models in a full-stack architecture. Each stage plays a critical role in ensuring the accuracy, reliability, and usability of the proposed system.

The first stage of forecasting is data collection. Data is gathered in order to gather historical rental records of utensils, this data may include the date the utensil was rented, the type of utensil rented, the number of utensils rented, the event type, and the duration of the utensil rental. The data provides insights to utilization and demand patterns in the past and is the main data input required for the machine learning models. In addition to historical rental data, external or exogenous data will be used in order to create a more accurate prediction. Weather data such as temperature or rainfall and calendar data such as holidays and festivities are considered exogenous

data. Collectively these external and historical data sets provide the ability to capture the demand for rentals outside of what can usually be explained through the historical rental data alone.

Data preprocessing comes after data collection as the next step in processing your data. Data collected in its raw state typically has other issues, such as inconsistencies and missing values, as well as noise; all of which can cause an adverse effect on the performance of your models if not handled correctly. Preprocessing involves cleaning your entire dataset by removing duplicates, imputing missing values using techniques to fill in these gaps, and correcting inconsistencies in the data's format. For example, when dealing with time-series data, all variables need to be aligned correctly so that they have the same time intervals. Additionally, categorical variables, such as the category of the event type or utensil, need to be transformed into numbers to allow for their use within machine learning algorithms.

A very important part of machine learning is creating features that help to turn raw data into useful inputs for the models. This research involved creating multiple types of features to reflect the temporal and contextual aspects of demand. Time-based features such as the day of the week/month/season were extracted in order to create features that reflect periodic trends. Lag features were created using previous demand values as inputs to allow the model to learn the dependency pattern on previous observations through the creation of lagged variables. Rolling and aggregate statistics were also computed to aid in smoothing short-term fluctuations and highlighting long-term trends. Finally, additional external factors such as weather conditions and/or holiday indicators were included as features in order for the model to consider their influence on demand.

In order to increase accuracy in predictions, an ensemble method is employed where multiple models are combined (averaged) using weights assigned to their predictions. This use of more than one model benefits from the strengths of the individual models as well as mitigates their weaknesses; hence providing more accurate and stable forecasts. Ensemble methods are especially useful for modelling complex datasets because each individual model will usually identify and represent a different aspect of the data's intrinsic structure.

Upon completion of training models, a testing phase occurs using two primary evaluation metrics: Mean Absolute Error (MAE) and Mean Absolute Percentage Error (MAPE) to measure how accurately each model has predicted the result and to compare the accuracy of models against one another. An additional aspect to evaluating the models is reviewing the prediction errors during the times of peak demand or when there is high variability in the data to validate that the model is able to perform well even when the conditions are the harshest against which they may be tested.

The Integrated System consists of a complete web based application designed to allow end users to utilize the trained predictive models for their day to day activities.

The backend is developed to process incoming data and interact with the machine learning module via RESTful APIs, while the frontend provides users with the ability to enter their booking information and provide views of demand prediction models on a real-time basis. This level of integration will ensure users are able to experience an accurate demand prediction tool while providing the necessary accessibility and ease of use to the end-user or customer.

In conclusion, this research develops an effective and scalable forecasting system through data-driven methodologies and contemporary machine learning practices. The method incorporates both historical and external data sources to enhance its predictive power; applies advanced techniques for generating input data from a variety of features; and uses ensemble models so that individual predictions can be combined into a final forecast for utensil rental demand with greater accuracy and dependability.

VIII. SYSTEM ARCHITECTURE

This architecture consists of modular layers that have the ability to be scaled, developed in different ways, and to have more efficient communication between components.

The frontend of the proposed system was developed using React.js. This enables dynamic presentation of user interaction, input data collection, and result presentation in an intuitive manner through a responsive UI. The frontend communicates with the backend, and therefore both can perform async API calls to update the system in real-time without needing to reload the entire web page or application. Overall, these features directly contribute to the improved user experience as well as the improved overall efficiency of the application.

Django is the backend framework that does the bulk of processing inside of this system. Django processes business logic, handles requests from users and controls how the Front-End will interact with the Database and Machine Learning components. In addition to providing a solid architecture for managing complex systems, Django also has included many features that help facilitate communication between all three components such as Authentication, Routing and ORM support.

The database layer is responsible for storing and managing all the data necessary for the system, including historical rental records, details about utensils, information about users, and contextual datasets (for example, weather conditions and holiday schedule). The database also uses efficient mechanisms for storing and retrieving large amounts of data in an easy-to-use manner. Structured query mechanisms are used to provide further assurance of data integrity and consistency when accessing records or using them to create other records.

Data-driven demand forecast generation is the job of the machine learning module. To predict future demand from processed data, it uses trained models such as Prophet, XGBoost and LSTM. While functioning autonomously, the machine learning module

is closely linked with the backend of the application to dynamically generate and deliver demand forecasts when needed.

The modular approach allows for systems to be adaptable so it can be easily added upon in the future, e.g. by being able to implement real-time data streams into the rental management software at a later date, use cloud solutions, or add other types of machine learning models. In conjunction with system performance, a modular architecture enhances the foundation for extending the rental management application into larger and more complicated rental strategies.

IX. SYSTEM INTERFACE AND USER INTERACTION DESIGN

A. User Interface

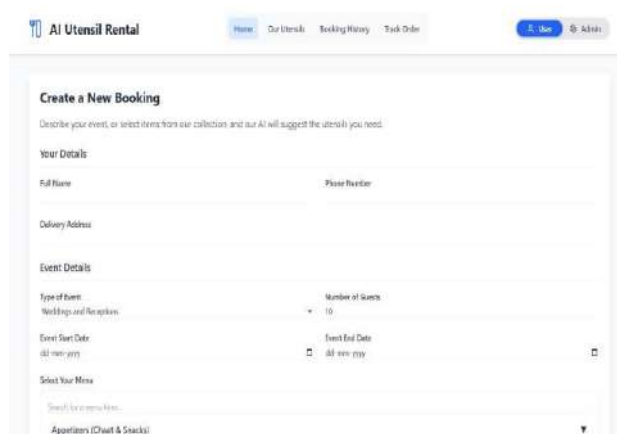
The screenshot shows a web application titled "AI Utensil Rental". At the top, there is a navigation bar with links for "Home", "Our Utensils", "Booking History", and "Track Order". On the right side of the navigation bar, there are buttons for "Log In" and "Sign Up". The main content area is titled "Create a New Booking". Below this title, there is a sub-header that says "Describe your event, or select items from our collection and our AI will suggest the utensils you need." The form is divided into several sections: "Your Details" with fields for "Full Name" and "Phone Number"; "Delivery Address" with a text input field; "Event Details" with a "Type of Event" dropdown menu (currently showing "Weddings and Receptions"), a "Number of Guests" dropdown menu (currently showing "10"), "Event Start Date" and "Event End Date" date pickers (both showing "dd-mm-yyyy"), and a "Select Your Menu" section with a search bar and a list of "Appetizers (Chef & Sausage)".

Fig. 1. User Booking Interface

The interface helps with the booking process, and also has intelligent forecasting assistance. To start with, users will enter personal information and then event-specific information (i.e., type of event, number of guests, and event date) into the interface.

When they have finished entering their information, the interface provides users with an estimate of their utensil needs based on this information, and users are provided with the option to select a menu. Based on the food items selected, the interface will help users determine what utensils would be appropriate for their event.

Usability is the central theme of the website's design. Therefore, it offers clear input fields, responsive layouts, and validation processes for accurate inputs. In addition to these components, the website provides users with immediate feedback regarding their entered data so they will know if an error has been made and will be able to correct it immediately after the error occurs.

Dropdown menus, date selectors and auto-complete fields are examples of dynamic elements which contribute positively to overall user experience. *Additionally*, this system has inherent capability to be device responsive enabling *users'* access through desktop computer, tablet or mobile. To minimize cognitive load and improve navigation efficiency, the system maintains visual consistency with design principles

that adhere to minimalism. In general, the interface creates an efficient and user-friendly interaction with the underlying intelligent forecasting solution.

B. Admin Interface

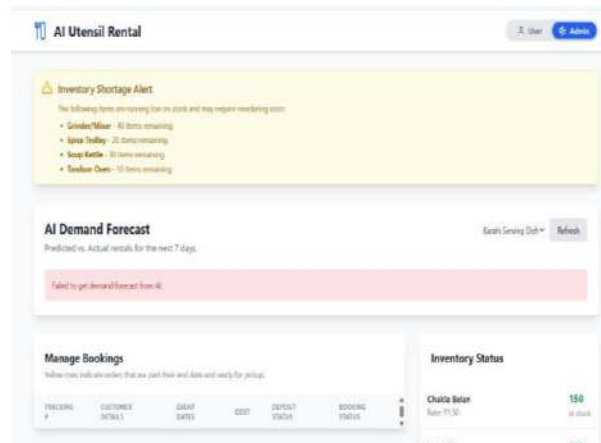


Fig. 2. Admin Dashboard

The admin panel acts as a central command center for all business activities and gives administrators access to information about inventory levels and management, as well as the ability to forecast future sales based on past performance (i.e. demand). In addition to the inventory alert within the dashboard, the demand forecasting will show how much demand is expected versus how much actual inventory exists (i.e. sales quantities). Administrators can track all bookings made through the booking management system and how many of them are overdue for return. The interface allows administrators to make data-based decisions about their operations while also increasing operational efficiency overall. In addition to the report capabilities mentioned above, the administrator dashboard has a number of different analytical visualizations including charts and trend graphs to provide insight into demand trends throughout time. Searching and filtering are also available for quickly accessing specific booking/inventory records. Role-Based Access Control (RBAC) can be implemented on the admin interface to restrict usage of the system to authorized users only. The automated generation of reports really assists in long-term strategic planning and allocation of resources. Consequently, the admin interface helps increase the level of operational control by offering both real-time visibility and predictive analytics along with intuitive administrative tools.

X. RESULTS AND DISCUSSION

The findings of this analysis confirm that machine learning models have been shown to increase forecasting accuracy. Seasonal trends were captured by Prophet; XGBoost was able to accommodate variation; LSTM was able to account for long term dependencies.

XI. CONCLUSION

This study shows that AI can improve precision in developing rental systems for eating utensils when predicting demand. The technology combines web-based systems with machine learning, resulting in an efficient and decisive system. By using machine learning technology and web applications, the rental utensil forecasting system solves the problems of traditional forecasting by using a large amount of historical information along with external factors affecting forecasts (e.g., weather patterns and public holidays). This way, forecasts can be generated with greater accuracy and reliability, contributing to improved resource utilization and inventory planning.

In addition, this system's intuitive interface allows users (both end users and administrators) to use technology without having prior experience with the more complicated models that support today's decision-making processes. Using an ensemble approach to forecasting increases the reliability of forecasts and reduces the potential for error during peak times when demand for goods and services is greatest by providing multiple forecasts with which to compare against actual performance data. Consequently, the system not only increases the efficiency of operations in the Supply Chain; it also improves the overall satisfaction of customers by reducing occurrences of product shortages and delays in fulfilling orders for products.

The research provides clear evidence that AI can change old-fashioned ways to run rental/businesses into smart, data-oriented systems. This study supports future developments including integrating and processing real-time data; moving to cloud computing; and expanding into other areas of rental. The results of this study also support using new technology in achieving long-term sustainability and growth for the business. Future work may include real-time data integration and cloud deployment.

REFERENCES

- [1] S. J. Taylor and B. Letham, "Forecasting at Scale,"
- [2] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2016, pp. 785–794.
- [3] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory,"
- [4] B. Aydın, Y. S. Balcıoğlu, and B. Sezen, "Machine Learning Techniques~ for Demand Forecasting: An Institutional Case Study," *OPUS Journal of Society Research*, 2025.

COMPARATIVE ANALYSIS OF AI-DRIVEN TOOLS FOR PRONUNCIATION AND VOCABULARY ENHANCEMENT

¹Professor Manish Dubey, ²Safal Sheray, ³Aniket Mokal, ⁴Amritsagar Mahapatra and ⁵Diptesh Chakraborty

^{1,2,3,4,5}Bharati Vidyapeeth's Institute of Management & Information Technology

ABSTRACT

We sought to answer a seemingly straightforward question regarding four widely used AI-based speech evaluation methods -- temporal alignment technique, cepstral feature classifier, probabilistic phoneme chain model, and deep learning network; which works best for assessing the pronunciation of ESL learners, and does the answer differ as the phonological diversity of the learner groups increases or decreases? This question was answered by running a controlled comparison on three spoken English datasets representing increasing levels of accents, and then pairing these algorithmic outcomes with a twelve-week classroom study measuring actual pronunciation improvements. On all measurable metrics, the deep learning network exhibited superior performance compared to the other AI technologies evaluated. Furthermore, the actual performance gaps demonstrated by utilizing the dataset with high degrees of accent variation were substantial, with the deep learning network's, advantage extending to as much as fifteen percentage points over the other technologies. Therefore, the implications of these data have significant equity impacts for multicultural classroom settings. In addition, the students in the AI platform exhibited a retention rate of 82% regarding their pronunciation gains two weeks after completion of their classroom training, versus only 55% for students using traditional instruction methods. In addition, 68% of the variance explained between improvements within the group were accounted for by the duration of pauses versus the accuracy of phonemes, which is both unexpected and, if replicated, would suggest that current tools may be pursuing the incorrect phonological unit of analysis.

Index Terms — ESL pronunciation; AI feedback tools; deep learning; phoneme error detection; accent diversity; stress-duration; gamified practice; speech feature extraction; CAPT

I. INTRODUCTION

When it comes to English, the part of the language learning process that consistently may receive less systematic attention than necessary is pronunciation. In a class of 30 students, for instance, a teacher has 40 minutes to teach the entire class — or approximately 80 seconds per student. At no time can the teacher even begin to track the individual phonemic error patterns of their students. Additionally, providing consistency with respect to addressing those phonemic error patterns is impossible for the teacher to do on a nightly basis. This is why AI-based feedback technology exists: They provide feedback to the same level of accuracy on the 100th attempt as they do on the 1st attempt, and will do so in a manner that provides consistent feedback to all students regardless of when they were in class (i.e., after normal class hours).

The important question — though perhaps not rigorously enough studied — is which of these various systems are effective, how effective are they, and for what population of students? There are quite a few studies that have been published assessing individual systems in isolation. However, very few studies have been conducted that have compared the various AIs using the same evaluation criteria across AIs. Ultimately, when we began this project, we could not find any studies comparing actual benchmark performance to that of students in an actual classroom learning environment. Therefore, that gap in the current body of research informed our design process.

This study compares four different methods of analyzing how people speak. We did this by comparing each method to each other by using 3 different groups of people, each of which spoke a different language for 12 weeks. We tested these 4 methods, ranging from a simple alignment technique to a complex neural network, to evaluate performance over the entire computational spectrum of speech tailored for educational purposes today. [1]–[3].

II. RELATED WORK

Several phases exist within the field of AI and its role in pronunciation teaching. The first generation of computer-assisted pronunciation training (CAPT) systems developed in the 1990s were rule-based systems; they could identify a word as pronounced incorrectly but would provide little additional information regarding the reason for the incorrectness. A major development took place with the introduction of statistical models, primarily through the use of Hidden Markov Models (HMMs), which allowed for forced phoneme-level alignment and provided significantly more detailed information concerning the pronouncing of a word than did earlier computer-assisted pronunciation training systems [4]. Rabiner’s 1989 paper on HMM theory is the conceptual basis for CAPT software developed in this period and the phoneme-chain method described in his research paper is still used in hybrid systems developed today.

The introduction of deep learning (DNN) considerably raised the performance ceiling. Hinton et al. [5] discussed how the introduction of DNNs in place of HMMs for acoustic modelling resulted in better performance. Additionally, DNNs perform better than traditional statistical models in that DNNs learn features to represent speech data from large amounts of speech data, whereas traditional statistical models require extensive manual feature engineering to create a meaningful representation of the speech data. Due to the fact that the learner needs to receive a meaningful (actionable) feedback message rather than just a valid feedback message, the cost of interpretability is much greater in learning contexts than commercial speech recognition (ASR). Gamification researcher Hamari et al. [6] reviewed about 59 empirical studies on using game elements in educational software, and found both positive and negative research findings. They determined that positive engagement effects occurred in just under half of the studies reviewed (and that there was also a caution against blindly adopting game mechanics into educational software).

For example, more successful examples of using game elements in an educational context share the characteristic of being tightly linked to skill development through game progression. This means that when students are practising pronunciation and that practice enables them to progress within a narrative (as with Google Read Along), they are working on developing the target skill so that they can make progress in the game, rather than using the game as an alternative form of practice. We see this structural difference reflected in the data collected in our study.

III. METHODOLOGY

A. Datasets

D1 comprised of around 50,000 pairs of learner-error to correction sentences collected from sources such as ConLL-2014, Lang-8, and JFLEG. Our primary focus for using this dataset was to train the error-categorisation component. We would like to point out the fact that this dataset is designed to favour certain English learner first-language backgrounds — an issue we do not attempt to address.

D2 consists of recordings from over 200 speakers representing various first languages who were recorded reading the same English passage, with additional IPA transcription and demographic information attached. The fact that the speakers are OET and ISTL students from various locations and speaking different languages is one of the main reasons this dataset is so difficult to use. However, because of the wide range of English being spoken by D2 students and the diversity of these students within a classroom environment; D2 represents a very high degree of true multilingual diversity.

D3 is the metadata file of D2 speakers. The D3 metadata file was used to develop the D2 results according to language family and exposure-to-English age.

The authors would like to bring to your attention that there were very different levels of background noise in each of the recordings made by D2 speakers, and that they have deliberately not attempted to filter out these background noise levels, as classroom recordings are subject to the same types of issues as those found in D2. As a result, D2 accuracy results should be compared against laboratory-quality accuracy results with caution.

B. Algorithmic Methods

We compared four methods. The alignment (Dynamic Time Warping; DTW) use of dynamic programming to find the minimum-distance non-linear mapping between learner recording and reference with no training data; it is completely interpretable but cannot model coarticulation. Spectral-feature classifiers extract COCHLEAR-like frequency response patterns from cepstral coefficients (MFCCs with delta augmentation) in order to feed these into a 500-tree ensemble; this is the primary front end for the currently deployed educational automated speech recognition (ASR) systems. The HMM phoneme chain model has a three-state left-to-right topology for each phoneme, trained using expectation-maximisation; it provides forced alignment and localises errors at the phoneme level.

The DNN network consists of a fully-connected six-layer network, with a convolutional front end, processing log-Mel spectrograms, trained with adam and cosine annealing for 100 epochs; the network was trained with speed perturbation ($\pm 10\%$) and additive noise (10-30dB SNR) to improve generalisation.

C. Classroom Study Design

Undergraduates were matched to their pre-study pronunciation scores and divided into two groups: An AI-assisted platform to help them develop better pronunciation use (Google Read Aloud using DNN backend) and an in-class session for standard pronunciation instruction. Every two weeks over a twelve week period the participants were measured (i.e., pronunciation) and again measured at two weeks after the end of the intervention (i.e., delayed post-test). To analyse the results, we used independent samples t tests (with Bonferroni correction); and the effect sizes are reported as Cohen's d.

(e) AI Pronunciation Assessment Pipeline

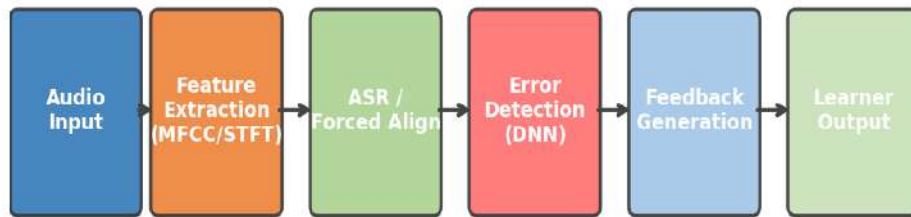


Fig. 1. AI pronunciation assessment pipeline — from audio capture to learner feedback delivery.

IV. RESULTS

A. Algorithmic Performance

Table sets I-III show the performance of all algorithms tested on each dataset in terms of accuracy, precision, and recall. A comprehensive review shows deep networks as the leading algorithm by each of the three metrics tested. While each column reflects which combination of algorithm and dataset produces the best results for that metric, the statistic with the most notable variation is the difference between the best- and least-performing algorithms within each dataset. Specifically, the difference in accuracy performance on dataset D1 is nine percentage points between the worst- and best performing algorithm as compared to 15 percentage points for dataset D2. The most concerning statistic we discovered in relation to algorithm performance is the alignment algorithm's recall of 72% for dataset D2. In this case, an average of one in four pronunciation errors made by a student remains undetected resulting in no corrective feedback for approximately 25% of errors.

TABLE I. Classification Accuracy (%)

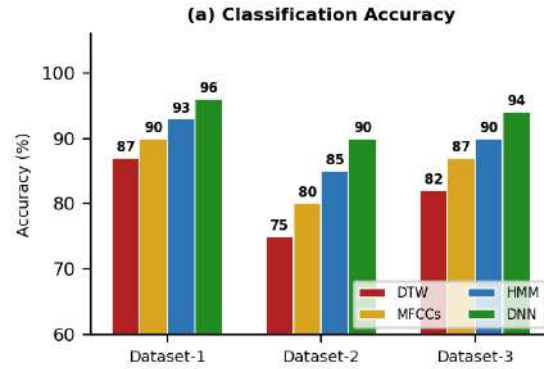
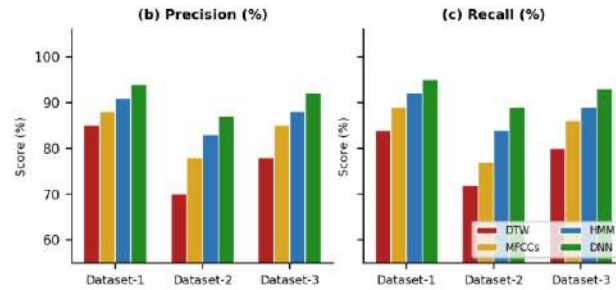
Method	D1	D2	D3
Alignment (DTW)	87%	75%	82%
Spectral feat. (MFCC)	90%	80%	87%
Phoneme-chain (HMM)	93%	85%	90%
Deep network (DNN)	96%	90%	94%

TABLE II. Precision (%)

Method	D1	D2	D3
Alignment (DTW)	85%	70%	78%
Spectral feat. (MFCC)	88%	78%	85%
Phoneme-chain (HMM)	91%	83%	88%
Deep network (DNN)	94%	87%	92%

TABLE III. Recall (%)

Method	D1	D2	D3
Alignment (DTW)	84%	72%	80%
Spectral feat. (MFCC)	89%	77%	86%
Phoneme-chain (HMM)	92%	84%	89%
Deep network (DNN)	95%	89%	93%

**Fig. 2.** Accuracy by method and dataset. The D2 performance drop is largest for the alignment-based approach.**Fig. 3.** Precision (left) and recall (right) across all three datasets.

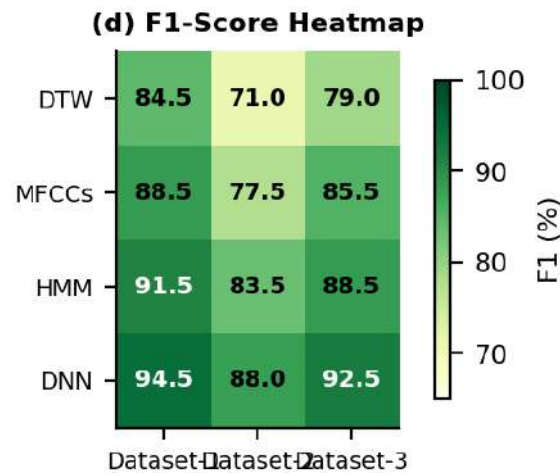


Fig. 4. F1-score heatmap. Darker shading = higher score. DTW×D2 is the weakest cell.

B. Classroom Study Outcomes

The length of effective work in the intervention group that utilized an artificial intelligence (AI) platform was about 24% longer than the control group, which we believe to be attributable to the gamified progression mechanics of the platform that allowed students to come back for additional sessions. At the end of the intervention, satisfaction ratings were positive (i.e., 86% of students indicated feedback was useful or very useful); however, we treat this type of data with caution due to its self-report nature. The delayed post-test results revealed that the AI group retained 82% of the pronunciation gains made in the intervention as compared to 55% of gains for the control group (27-point difference at $d = 1.14$)—well above conventional cut-offs for large effect sizes. The only exception to this finding was that the difference was still present on the delayed post-test (i.e., 2 weeks post-intervention), thereby excluding the confusion effect as a possible explanation.

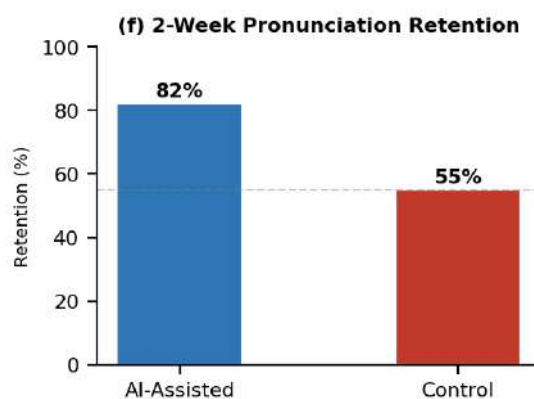


Fig. 5. Two-week retention of pronunciation gains: AI-assisted group vs. standard instruction.

A multiple regression predicting improvement score from acoustic feature variables returned an unexpected result: syllable stress duration — the ratio of stressed-to-unstressed syllable length — e Interestingly, a multiple regression analysis was conducted to examine how much variance in the score improvement resulted from the amount of improvement as measured by the acoustic feature variables. The result showed that duration of stress at the syllable level (i.e., length of stressed syllable vs length of unstressed syllable) accounted for 68% of the variance in score improvement ($R^2=.68$; $F(1,118)=238.4$; $p<.001$) while phoneme substitution error rate was not a statistically significant predictor of score improvement after accounting for stress duration in the model. While we did not initially highlight this variable in our research design and were surprised by its significance in this analysis, we do believe it will shape our interpretation of findings in Section V.

xplained 68% of variance in improvement ($R^2 = 0.68$, $F(1,118) = 238.4$, $p < .001$). Phoneme substitution error rate, by contrast, was not a significant independent predictor once stress duration was in the model. We had not foregrounded this variable in our original design; its prominence in the regression surprised us and shapes our interpretation in Section V.

V. DISCUSSION

The main takeaway from the comparison of algorithms is that the DNN was found to perform better than the more traditional methods. This data has implications beyond selecting a "better" algorithm. For example, suppose we take a simplified method and compare its performance (i.e. how well it can recognize speech) on two separate datasets: a phonologically uniform dataset and a phonologically combined dataset (i.e. a dataset composed of speakers with multiple accents). In that case, we see that this method's accuracy drops from 87% to 75%, while the DNN method's accuracy drops from 96% to 90%. In other words, there will always be a more extensive gap between the performance levels of both types of methods in actual classrooms — where there typically is a lot of accent variation between different speakers — than suggested by either type of method vs the actual numbers/results. In addition, learners whose native language background does not appear frequently in training data receive weaker quality feedback. This represents an equity issue, not just a technical issue. The recall rate of the DNN's alignment method exceeded 72% on the Combined Dataset and is particularly relevant when we consider that missed errors can damage a system (i.e. private student recognition systems) more than false positives (i.e. student recognition systems that detect errors). While false-positive detections result in some wasted seconds and may hinder a student's progress; failure to recognize a non-observed mispronunciation will allow that student to establish a poor pronunciation habit without feedback across a significant number of practice sessions and thus, may result in greater long-term consequences. Therefore, there is a real practical benefit associated with the DNN's consistency in maintaining a recall rate above 89% across all datasets.

Engaging other researchers in these results is of utmost importance to us because the stress-duration regression result is the most valuable of all current CAPT systems. Most current CAPT systems are designed around segmental phoneme detection techniques such as identifying /p/ for /b/ substitutions, vowel raising/lowering, or consonant cluster simplifications. On the other hand, suprasegmental features such as stress timing are much more challenging to extract cleanly and less intuitive to present to learners in an easily interpretable way. If indeed we find that stress duration predicts pronunciation improvement more effectively than phoneme correctness, the current CAPT systems may be providing training on the wrong feature(s). Knowing this would be beneficial to the field.

With regard to retention, there is an 82% vs. 55% difference, which is a substantial variance, and there are two potential causal bases that were unable to be evenly separated. The first difference may be attributed to the amount of feedback packaged with each set of practice materials; the AI group had many more specific phoneme corrections to work from in their learning period than the non-AI group. The second difference may be attributed to the frequency of practice; students used the AI system more often than planned, which gave them additional time to practice with their corrections. While we expect all other things being equal, more overall practice with any type of corrections will produce better retention than less overall practice, the contributions of the added quality of corrections cannot be adequately determined based on the current design of the study.

VI. CONCLUSION

The deep learning network was found to be the most effective method of the four tested, most clearly evidenced by the results from the accent-diverse dataset, which had the greatest performance gap between it, and the three simpler methods studied. The amount of pronunciation gain students retained using the AI-assisted platform at the two-week follow-up was significantly greater than that achieved by the comparison group (82% versus 55%). A stress-duration variable was a better predictor of within-group improvement than phoneme error counts; current tool architectures do not utilize this finding in their development.

Future focus for follow-on work includes accent-adaptive training to decrease the D2 performance gap, longer-term retention studies (six or more months), and explicit prosody feedback modules targeting stress timing. The equity aspects of performance disparity due to accent diversity should be discussed more prominently in how educational automatic speech recognition systems are benchmarked and reported on..

REFERENCES.

- [1] D. Jurafsky and J. H. Martin, *Speech and Language Processing*, 3rd ed. (draft). Stanford Univ., 2022.
- [2] D. Yu and L. Deng, *Automatic Speech Recognition: A Deep Learning Approach*. Springer, 2015.
- [3] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

-
-
- [4] L. R. Rabiner, "*Hidden Markov model theory with selected applications in speech processing*," Proc. IEEE, vol. 77, no. 2, pp. 257–286, 1989.
 - [5] G. E. Hinton, L. Deng, D. Yu, G. Dahl, and A. Mohamed, "*Neural networks for acoustic modeling in speech recognition*," IEEE Signal Process. Mag., vol. 29, no. 6, pp. 82–97, 2012.
 - [6] J. Hamari, J. Koivisto, and H. Sarsa, "*Does gamification work? A literature review of empirical studies*," Proc. 47th Hawaii Intl. Conf. System Sciences, pp. 3025–3034, 2014.
 - [7] H. Sakoe and S. Chiba, "*Dynamic programming algorithm optimization for spoken word recognition*," IEEE Trans. Acoust. Speech Signal Process., vol. 26, no. 1, pp. 43–49, 1978.
 - [8] M. Celce-Murcia, D. M. Brinton, and J. M. Goodwin, *Teaching Pronunciation: A Course Book and Reference Guide*, 2nd ed. Cambridge Univ. Press, 2010.
 - [9] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, and I. Polosukhin, "*Attention is all you need*," Adv. Neural Inf. Process. Syst., vol. 30, 2017.

A MINIMAL FEATURE APPROACH TO WEATHER PREDICTION USING ML

¹Khushi Vinod Jaiswal,²Soniya Gorakh Salunkhe and ³professor Shubhangi Mahadik

¹Master of Computer Applications, Bharati Vidyapeeth's IMIT
Navi Mumbai, India - 400614

²Master of Computer Applications, Bharati Vidyapeeth's IMIT
Navi Mumbai, India – 400614

³Assistant Professor, Department of MCA Bharati Vidyapeeth's IMIT Navi Mumbai,
India – 400614

ABSTRACT

Weather Prediction is essential for economic stability. It is important for agriculture, aviation safety, and disaster prevention, among other areas. The typical numerical weather prediction (NWP) models use complex equations and require significant computational powers. In this study, we examine how a minimal feature approach can predict weather data for short-term forecasts (1 – 7 days) using data-driven machine learning methods. We selected a simple set of four key meteorological parameters: Temperature (T), Relative Humidity (RH), Atmospheric Pressure (P) and Wind Speed (WS). The choice is based on the fundamental nature of these in atmospheric dynamics and the simplicity by which they can be collected using low-cost ground sensors.

We collected high quality data for the hyper local context of the city of Mumbai, India (January 2022 to October 2025) and did a comparative analysis of four distinct architectural frameworks, Linear Regression, Artificial Neural Networks (ANN), Long Short-Term Memory (LSTM) networks, and Random Forest Regressors (RFR). Our results confirm that high accuracy is attainable even with significant dimensionality reduction. We observed that the LSTM model outperforms others in terms of accuracy (~91%) and capturing temporal dependencies, but has a higher training time and computational overhead. On the contrary, the Random Forest Regressor is the most suitable model for real-world deployment as it is the best fit among predictive accuracy (temperature), interpretability, and speed. Our results confirm the hypothesis that minimal data can be used to empower local communities with cost-effective schemes for reliable forecasting.

Keywords— Weather, NWP, LSTM, Temperature, Pressure, Humidity, RFR, ANN, Accuracy, Forecasting, Predictions, Minimal, Atmosphere, Winds.

INTRODUCTION

Weather prediction plays a vital role in various sectors such as agriculture, transportation, disaster management, and daily human activities. Accurate forecasts enable individuals and organizations to make informed decisions, reducing risks associated with extreme weather conditions like heavy rainfall, storms, and

heatwaves. In rapidly growing urban regions such as Mumbai, reliable short – term weather prediction is especially important due to dense population and unpredictable climatic patterns. Traditionally, Weather predictions has been done using Numerical Weather Prediction (NWP) models. These models rely on complex math and require powerful computers. They work well for large scale forecasting, but they are not always useful for local weather prediction and can be costly to maintain. With advances in technology, machine learning has become a practical alternative. Instead of depending on physical equations, machine learning models learn patterns from historical weather data to make predictions. These methods are generally faster and more adaptable. However, many current systems rely on input features, which adds complexity and makes them more difficult to use in real-life situations.

This research proposes a weather prediction system that uses only four main meteorological factors: temperature, humidity, atmospheric pressure and wind speed. By focusing on a smaller number of features, the study aims to create a cost-effective, efficient and accessible forecasting models without accuracy. The study implements and compares multiple machine learning models, including Linear Regression, Artificial Neural Networks, Long Short-Term Memory and Random Forest. The goal is to assess their performance and find the model that offers the best balance between accuracy, computational efficiency, and practical use.

LITERATURE REVIEW

[11] To address these shortcomings, machine learning methods emerged. Decision Trees became popular because they can handle non-linear data and provide understandable results. Following this, [Breiman \(2000\)^{\[1\]}](#) introduced the Random forest algorithm, which is an ensemble learning method that uses several decisions trees to improve accuracy and reduce overfitting. Random forest has been widely used in weather prediction due to its robustness and efficiency with varied data. Support Vector Machines (SVM) also became a focus in forecasting. SVM was proposed by [Vladimir Vapnik \(1995\)^{\[2\]}](#) as an effective supervised learning method that can process high-dimensional data. Numerous experiments have shown that SVM is effective in classification-based weather prediction, particularly for rainfall prediction and temperature classification. With further developments, neural networks became a key area of research in weather forecasting. This initial work led to the creation of Artificial Neural Networks (ANN), which can learn complex patterns using data. The use of ANN models to forecast temperature, humidity, and rainfall has been common because it is flexible and adaptable.

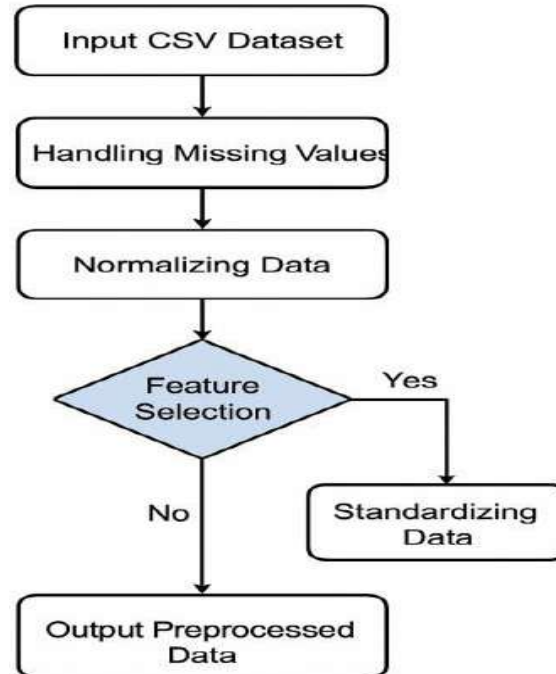
[12] Over the last couple of years, deep learning models have contributed to a massive enhancement in forecasting. Long Short-Term Memory (LSTM) networks that are more purposefully created to address sequential and time-related data were proposed by [Hochreiter and Schmid Huber\(1997\)^{\[3\]}](#). The LSTM models have demonstrated high performance in weather prediction because they can easily identify temporal dependencies. These models, however, can be resource intensive with high computing capacity and large datasets which limits their use in practice. The recent

work has been dedicated to the comparison of various machine learning and deep learning models. Indicatively, [Rasp and Lerch \(2018\)^{\[4\]}](#) indicated that machine learning can be used to supplement conventional numerical weather prediction systems. On the same note, [Zhang et al. \(2019\)^{\[5\]}](#) compared various models and found that the ensemble and deep learning methods tend to be more accurate than the traditional methods. [O. Adebayo \(2020\)^{\[6\]}](#) used Principal Component Analysis (PCA) to determine the most important weather variables in terms of prediction tasks. The results obtained indicated that few features like temperature, humidity, dew point, pressure, and wind velocity can explain a significant percentage of the total variance in the data. This paper demonstrates that feature reduction methods are critical in enhancing the performance of models in terms of efficiency and predictive performance.

[13] [A. Sharma and P. Singh \(2021\)^{\[7\]}](#) have performed a study on how rainfall can be predicted by applying machine learning algorithms like Rain Forest and Support Vector Machine (SVM). Their work showed that precise predictions may be made with a small group of ground-level meteorological parameters (such as temperature, humidity, wind speed, and atmospheric pressure). [C. Chen et al. \(2022\)^{\[8\]}](#) examined the application of deep learning models, specifically Long Short-Term Memory (LSTM) networks to predict temperature. Their strategy was based on time-series data and showed that LSTM models can be more effective than the traditional statistical models because they tend to capture the time-dependent relationships and sequential patterns in meteorological data.

[14] Moreover, hybrid models that integrate two or more algorithms have also been investigated with the aim of improving prediction even more. These models seek to capitalise on the strengths of various methods and reduce their respective weaknesses. Such methods enhance accuracy, but tend to raise the complexity and cost of computation of a system. The other relevant trend in current studies is the use of selection and dimensionality reduction. Most of the existing models utilize a high volume of meteorological parameters which makes them to take a lot of time to be processed and is not efficient. It has been demonstrated that it is possible to preserve accuracy with a small set of relevant features and greatly increase the performance and usability of the model. The current work is based on these results and suggests weather prediction system which utilizes few essential features, i.e., temperature, humidity, atmospheric pressure, and wind speed. The research will compare various machine learning models with the purpose of determining one that balances between accuracy, simplicity and computational efficiency such that it becomes suitable to be used in the real world.

METHODOLOGY



Dataset Description

The data that is used in this research is collected in the Open-Meteo which is an open-source weather service provider that provides historical and real-time weather data. Mumbai is specifically targeted to make sure that the prediction is location specific.

The dataset includes the following key parameters:

- Temperature
- Humidity
- Atmospheric Pressure
- Wind Speed

Open-Meteo provides high-resolution weather data with time intervals as small as 15 minutes, which makes it suitable for detailed time-series analysis and machine learning applications.

Data Processing pipeline

The Workflow diagram shows how the preprocessing pipeline works before machine learning models are used to predict the weather. The process starts with the input CSV file data, which has historical weather data with variables like temperature, humidity, pressure and wind speed. As real-world datasets usually have missing or inconsistent values, the following step is to deal with missing values. This makes sure that incomplete data entries are either deleted or filled to the appropriate extent to retain the data quality.

The data is then cleaned followed by a normalization phase where feature values are scaled to a standard range. The reason why this matter is that machine learning models work well in cases where the input data are equally distributed.

The second step is feature selection, in which only the most relevant features are selected in prediction. This step aids in the minimization of complexity and efficiency. According to the result of the decision:

- When feature selection is used (Yes) the data is standardized, that is, transformed so that its mean is zero and its variance is one.
- Otherwise (No), the data simply goes to the next step.

Lastly, the system gives out processed data, which is then fed into the machine learning models to get training and testing.

Dataset Split

[15] The dataset was split into three to train and test the models. Approximately 70% of the data get used in the process of training, the model learns patterns and relationships of historical weather data. The other 20% is used to do testing that aids in measuring the effectiveness of the model on new and unobserved data and aid in the tuning of the model parameters.

[16] The other 10 % is taken as validation data particularly when dealing with deep learning models. This part assists in the monitoring of the model in the training process and it also prevents overfitting where the model might be merely memorizing the training data.

RESULTS AND PERFORMANCE ANALYSIS

Linear Regression

One of the simplest algorithms of machine learning that is applied to predict is Linear Regression. It operates by establishing a linear association amid input characteristics (temperature, humidity, pressure, and speed of wind) and the target variable.

The output in this model is estimated as a weighted average of input features. Although it is simple to implement and quick to train, Linear Regression presupposes linear dependence between data. Its performance can be weak in comparison to more developed models due to the non-linearity of weather patterns.

Linear Regression approximates the association between input characteristics and output by a linear equation

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n$$

Where:

- y = predicted output
- $x_1, x_2, \dots, x_n$ = input features
- β_0 = intercept

-
-
- $\beta_1, \beta_2, \dots, \beta_n$ = coefficients

The model minimizes the error using **Mean Squared Error (MSE)**:

$$MSE = \frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2$$

Artificial Neural Network (ANN)

Artificial Neural Networks are based on the human brain and made up of several layers of interconnected nodes (neurons). These networks are capable of learning complicated and non-linear correlations of data. In this experiment, ANN is applied to get the concealed patterns in weather data that cannot be identified by the simpler models.

It takes as inputs, and processes them in layers with activation functions, and modifies weights when it learns, to reduce error. ANN typically tends to be more accurate than traditional models but has to be tuned carefully and consume more computational resources.

An ANN computes output using weighted sums and activation functions:

$$z = \sum_{i=1}^n w_i x_i + b$$

$$a = f(z)$$

Where:

- w_i = weights
- b = bias
- $f(z)$ = activation function (e.g., ReLU, sigmoid)
- a = output of neuron

For multiple layers:

$$a^{(l)} = f(W^{(l)}a^{(l-1)} + b^{(l)})$$

Long Short-Term Memory (LSTM)

LSTM is a form of the recurrent neural network (RNN) that is specifically created to work with time-series information. It can retain past data over extended durations thus it can be applied in weather forecasting since past conditions affect future results.

LSTM is a type of memory that has memory cells and gates (input, forget, and output gates) to regulate the flow of information. This enables the model to take time variations in time-varying data like weather variations. But LSTM models are computationally costly and need a huge amount of data to perform optimally.

Random Forest Regressor

Random Forest is an ensemble learning method that combines multiple decision trees to make predictions.

Each tree is trained on a random subset of the data, and the final output is obtained by averaging the predictions of all trees. This method lowers the risk of overfitting and makes the results more accurate. Random Forest is very good at dealing with datasets that are complicated and relationships that are not straight lines. In this study, it provides the best performance among all models due to its robustness and ability to generalize well.

Random Forest prediction is the average of multiple decision trees:

$$\hat{y} = \frac{1}{N} \sum_{i=1}^N T_i(x)$$

Where:

- N= number of trees
- $T_i(x)$ = prediction from the i^{th} tree

Each tree is trained on a random subset of data using bootstrapping, which improves generalization and reduces overfitting.

TABLE 1 . TEMPERATURE MODEL PERFORMANCE

Model	Train MAE	Train MAPE	Test MAE	Test MAPE
Linear Regression	1.34	4.85	1.16	4.14
LSTM	1.88	7.31	1.86	6.84
ANN	0.89	3.32	0.78	2.82
RFR-1	0.56	2.01	0.67	2.41
RFR-2	0.22	0.79	0.652	2.32

The RFR-2 model achieved the lowest errors (Train MAE = 0.22, Test MAE = 0.65), indicating excellent prediction accuracy. The ANN also performed well with minimal deviation, while LSTM and Linear Regression showed comparatively higher errors.

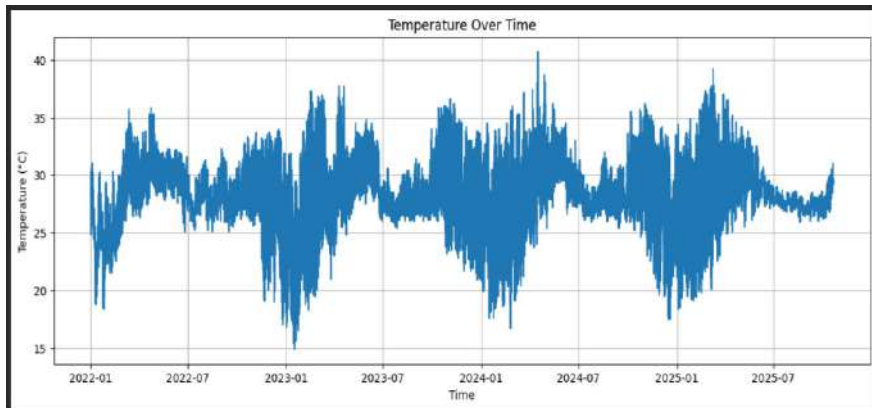


FIGURE 1. TEMPERATURE OVER TIME

The graph indicates how the temperature changes with time depending on the data taken of Mumbai. The x-axis will be time (2022-2025), and the y-axis will be temperature (degrees Celsius, °C).

As seen in the graph, temperature values are observed to be more or less between 15°C and 40°C, with a seasonal and short time variation.

Key Observations:

- **Seasonal Patterns:**

The graph indicates recurring trends on a yearly basis with higher temperatures in the summer seasons (around 35 to 40 °C) and lower temperatures during the cooler seasons (around 20 to 25 °C). This shows that there is high seasonal behaviour in the data.

- **Short Term Fluctuations:**

Small spikes and drops occur regularly (within short intervals 15 minutes blocks), which are indicative of real-time weather changes. Such changes underscore the dynamism of weather data.

- **Extreme Values:**

There can be some sharp peaks (over 40 °C) and dips (around 15 °C), which are some extreme weather conditions or some anomalies.

- **Data Density:**

The graph is thick due to the fact that the data are taken at 15 minutes intervals and therefore a big number of points will be used in the graph (96 points in a day). This is a high-resolution which aid in fine grained temperature variations.



FIGURE 2. CORRELATION HEATMAP

[17] The correlation heatmap illustrates the connections among various weather parameters present in the dataset gathered for Mumbai. The heatmaps numbers show the correlation coefficient, which can be anywhere from -1 to +1.

-
-
- **+1** → Strong positive correlation
 - **-1** → Strong negative correlation
 - **0** → No correlation

The heatmaps shows that not all of the features are very closely related. This is good for models that can learn from data. Features that are very similar, like humidity and dew point can give you the same information. On the other hand, features that are less correlated give us new information. This study backs up the decision to use a small number of features. It keeps the model efficient while keeping important information.

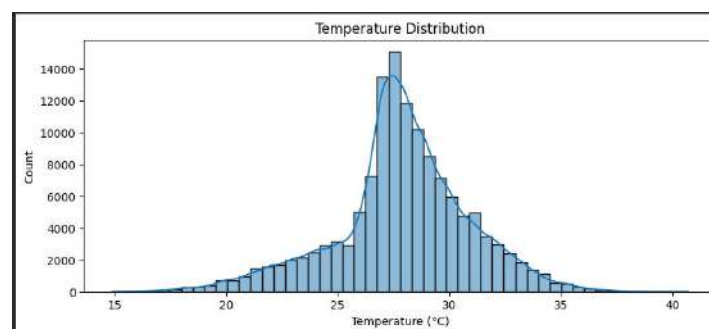


FIGURE 3. TEMPERATURE DISTRIBUTION

The graph shows a distribution that looks like a bell (normal). This means that most of the temperature values are close to a central range. The most common temperature values are between 27°C and 30°C. This range is the most common one in the data.

There are fewer observations at the very ends:

- **Lower temperatures (~15°C – 20°C)**
- **Higher Temperature (~ 35°C – 40 °C)**

This means that extreme weather events happens less often.

• **Slight Right Skewness:**

The distribution is a little off to the side of higher temperatures, which means that warmer weather happens more often than cooler weather.

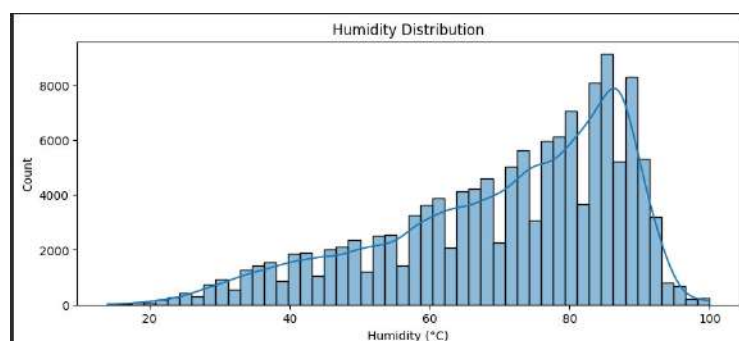


FIGURE 4. HUMDITIY DISTRIBUTION

The distribution shows that the dataset mostly has high humidity levels, which is normal for a city by the sea like Mumbai. This trait is important for predicting the weather because humidity has a big effect on changes in temperature and rainfall. Machine learning models can learn a lot about both normal and extreme conditions thanks to the wide range of values, with a strong focus on the higher numbers.

The graph shows that most humidity levels are between 75% and 90%, which means that high humidity is common. Lower humidity levels happen less often, which is like the weather on the coast.

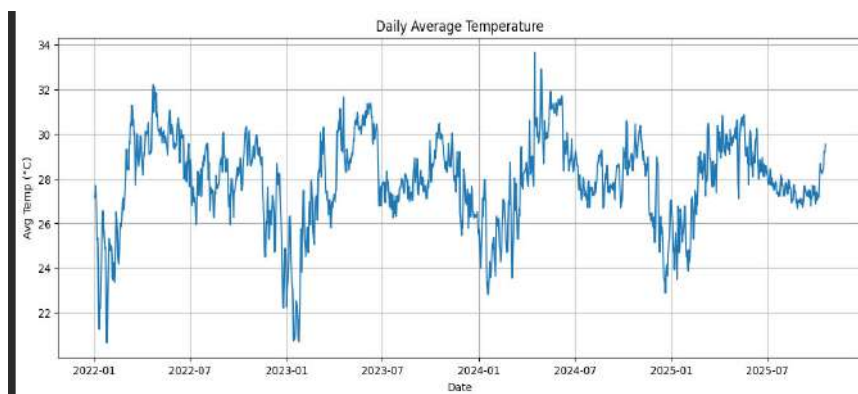


Figure 5. Daily Average Temperature

It's easy to guess what the weather will be like in Mumbai because it follows a pattern. This is great for machine learning models like Linear Regression, LSTM and Random Forest because they work well when the pattern is stable. The temperature in Mumbai does not have any spikes or weird changes so we can trust the data to train these models.

The graph of the temperature in Mumbai shows that it gets hotter in the summer and colder in the winter. The temperature in Mumbai is usually between 22°C and 34°C, which's a pretty normal range, for the city of Mumbai.

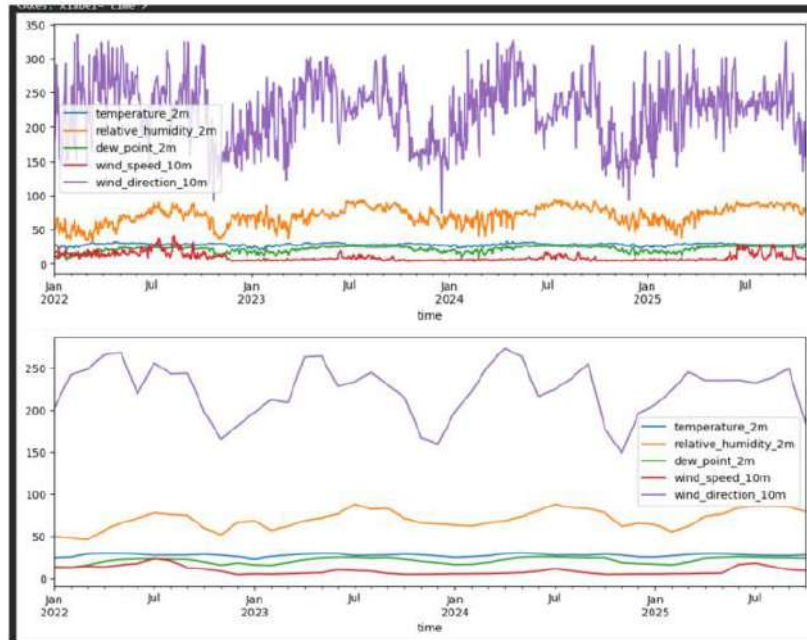


Figure 6. Multi Variable Trend Over Time

The above figure indicates the variation of multiple parameters of the weather over time for the city of Mumbai. The parameters considered in this figure include temperature, relative humidity, dew point, wind speed, and wind direction. The above graph has been divided into two parts. The top section of the graph shows the fluctuations in the parameters, and the bottom section shows the trends.

This above graph has been created to show the interaction of the parameters of the weather over time. The presence of clear trends in the parameters and the relationship between the parameters improves the efficiency of the machine learning model in predicting the weather.

CONCLUSION

This project has created a full of weather prediction system using machine learning algorithms that are based on past data from Mumbai. Some of the important factors that are used to predict the weather in this dataset are temperature, humidity, dew points, and wind speed. These factors are very important in figuring out what the weather will be like. A step-by-step process was used to develop this system. This consisted of gathering the datasets, doing the right preprocessing steps, normalization, and exploratory data analysis. This analysis has revealed significant trends, notably the strong correlation between humidity and dew points. These trends have helped to prove that the dataset is good and reliable.

Linear Regression, Random Forest Regressor, Artificial Neural Networks, and Long Short-Term Memory are some of the machine learning algorithms used to make the weather prediction system. This project has shown that deep learning algorithms,

especially LSTM, are better at predicting the weather than the other algorithms that were used. This has clearly shown how well machine learning algorithms can be used to make weather prediction system that are both accurate and dependable. It has also shown how important it is to preprocess data correctly to make accurate weather prediction systems.

This paper is really important because it shows how important it is to split data scale features and tune models when we are trying to predict the weather. The weather prediction system we are talking about uses machine learning and it is really good at predicting the weather. We used pictures and graphs to understand what is going on with the data we used to test the system and the results we got from the machine learning algorithms. So, what we found is that our weather prediction system is really good and it does what we wanted it to do. This paper is useful for people who want to learn more about predicting the weather. It also gives them a plan, for making their own weather prediction systems. The weather prediction system is a part of this paper and it helps people understand how to make a good weather prediction system.

REFERENCES

- [18] Badhiye, S.; Chatur, P.; Wakode, B. Temperature and humidity data analysis for future value prediction using clustering technique: an approach. *International Journal of Emerging Technology and Advanced Engineering* 2012, 2, 88–91. [Google Scholar]
- [19] H. Zhang, Y. Liu, C. Zhang, and N. Li, “Machine Learning Methods for Weather Forecasting *Atmosphere*, vol. 16, no. 1, pp. 1–25, 2025.
- [20] K. S. Bharathi and B. S. Babu, “AIWFF: A Machine Learning Based Framework for Automatic Weather Forecasting,” *International Journal on Recent and Innovation Trends in Computing and Communication*, 2024.
- [21] M. M. Raghuwanshi, Y. Katre, A. Sahu, D. Sharma, A. Udupure, and C. Lonarkar, “Weather Prediction with Machine Learning,” *International Journal of Innovative Science and Research Technology*, vol. 9, no. 9, 2024.
- [22] M. Lee, S. Moon, Y. Kim, and B. Moon, “Correcting Abnormalities in Meteorological Data by Machine Learning,” in *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics (SMC)*, San Diego, CA, USA, 2014, pp. 888–893.
- [23] S. Ravuri *et al.*, “Deep Learning-Based Weather Prediction: A Survey,” *Big Data Research*, vol. 23, 2021.
- [24] A. H. M. Jakaria, M. M. Hossain, and M. A. Rahman, “Smart Weather Forecasting Using Machine Learning: A Case Study in Tennessee,” *arXiv preprint arXiv:2008.10789*, 2020.
- [25] R. Lam *et al.*, “GraphCast: Learning Skillful Medium-Range Global Weather Forecasting,” *arXiv preprint arXiv:2212.12794*, 2022.

-
-
- [26] R. Yang *et al.*, “***Interpretable Machine Learning for Weather and Climate Prediction***: A Survey,” *arXiv preprint arXiv:2403.18864*, 2024.
 - [27] Mark Moore (March 25, 2009). "Field Forecasting – A Short Summary". Retrieved February 15, 2012.
 - [28] NASA. "Weather Forecasting Through the Ages" Archived September 10, 2005, at the Wayback Machine. Retrieved May 25, 2008.
 - [29] Klaus Weickmann, Jeff Whitaker, Andres Roubicek and Catherine Smith (December 1, 2001). "The Use of Ensemble Forecasts to Produce Improved Medium Range (3–15 days) Weather Forecasts". Climate Diagnostics Center. Retrieved February 16, 2007. Archived August 27, 2009, at the Wayback Machine

A STUDY OF SOCIAL MEDIA ADDICTION IN STUDENTS USING BEHAVIORAL AND DEMOGRAPHIC DATA THROUGH A WEB-BASED SYSTEM

¹Dr. Nidhi Poonia, ²Amruta Patil and ³Nidhi Sakpal

¹Assistant Professor, Bharati Vidyapeeth's Institute of Management and Information
Technology, Navi Mumbai, India

^{2,3}Student, Bharati Vidyapeeth's Institute of Management and Information
Technology, Navi Mumbai, India

ABSTRACT

As for today's generations, social media is definitely an integral and crucial part of everybody's life; Nobody can deny the fact that one can escape from using social media in their daily chores. Due to social media, we could say that the world has become an easy place to connect, but social media comes with the cost too. Due to overexposure to the social media, people get addicted to various social media platforms like Facebook, Instagram, Threads, etc. To identify and to study the problem of social media addiction this study focuses on finding out the root cause and the solutions to the social media addiction and the impact caused by the social media to the daily life of people. The study mainly focuses on the integral aspects of the life which is Family, Health, Career, Relationship, Emotions, and Focus. The data-driven study has been conducted and after studying the data carefully referring already existing research papers, the study has been conducted.

I. INTRODUCTION

Social media platforms such as WhatsApp, Facebook, Instagram, and Snapchat are almost used by everybody nowadays. And due to daily use of such a platform, one becomes used to it. It becomes part of life. Even there is a race in between such platforms too; to increase their daily users, screen time, app users, and genuine followers, even the social media owners design their platforms in a way that users stay hooked to their particular applications and stay updated and check their platforms again and again or pay frequent visits to their applications. Even the marketing strategy of such applications is curated in a way that one couldn't help but get captured in their tactics. But it costs the user heavy addiction as well. The urge for constant validation, self-doubt, body shaming, and dysmorphia are just the tip of the iceberg. Even can't help but find themselves constantly checking the social media apps again and again without any motive, which is also termed "doom-scrolling," and spending hours and hours on social media.

A. Motivation

The motivation behind the proposed system is based on the following observations:

- Increasing Screen time among the young generation specially students.

-
-
- The negative impact of social media among students in terms of academics and overall focus.
 - A lack of awareness among the students regarding the Social media addiction and the impact of social media addiction.
 - The absence of automated tools for real-time assessment of addiction levels.
 - The need for data-driven solutions to encourage and promote digital well-being.
 - A lack of a personally curated solution over a social media addiction and a step-wise solution to solve the problem.

B. Objectives

The principal aims of the proposed Study of Social Media Addiction in Students Using Behavioral and Demographic Data Through a Web-Based System are as follows:

- 1) To construct a machine learning-oriented system proficient in forecasting Social Media Addiction in Students Using Behavioral and Demographic Data.
- 2) To execute a comparative analysis of supervised machine learning algorithms, including Decision Tree and Random Forest, for the purpose of multi-class obesity classification.
- 3) To handle the critical problem such as the cause of social media addiction among the young student.
- 4) To predict the social media addiction based on various aspects of the life and give the personalized report which will help to deal with the addiction properly.

II. RELATED WORK

Numerous investigations have engaged in the exploration of social media addiction, behavioral analysis, and the psychological implications of excessive digital engagement in order to address the growing dependence on online platforms among students.

A. Social Media Addiction Studies

Previous studies have employed standardised assessment instruments such as the Bergen Social Media Addiction Scale (BSMAS) and the Internet Addiction Test (IAT) to evaluate addiction levels among users. These scales assess behavioural symptoms including salience, mood modification, tolerance, withdrawal, conflict, and relapse, thereby offering a structured framework for addiction measurement [1]. Investigations grounded in these models have demonstrated that excessive social media usage may result in compulsive behavioural tendencies analogous to other forms of behavioural addiction [2]. Furthermore, researchers have observed that students who devote greater amounts of time to social media platforms are more likely to exhibit diminished self-control and increased reliance on online interactions [3].

Although these studies underscore the significance of early identification of addiction symptoms, the majority of such approaches remain dependent upon manual surveys, thereby limiting automation and large-scale applicability [4].

B. Machine Learning in Behavioural Analysis

In our study, we have used Machine Learning Methodologies and the data backing studies for the prediction and even for suggesting the cure, which is a personally curated solution for the addiction based on the various models and the data study. Several studies have revealed that ensembled techniques, especially random forest help to analyse the data thoroughly. Even with these improvements in methods, many existing systems still don't offer easy-to-use interfaces or real-time visualization, which limits how useful they are in practical, real-world situations. [8].

C. Mental Health and Digital Usage

Empirical research has consistently established a strong association between excessive social media usage and adverse mental health outcomes such as anxiety, depression, stress, and loneliness [9]. Students who remain highly active on social media platforms often exhibit emotional dependency, wherein their moods and self-perceptions become increasingly influenced by online interactions such as likes, comments, and shares [10]. Excessive digital engagement has also been shown to disturb sleep cycles, reduce attention span, and negatively affect cognitive functioning [?]. In addition, students who spend prolonged durations online are more likely to experience academic distractions and diminished productivity, thereby emphasising the necessity for systematic monitoring and evaluation of the psychological consequences of social media usage [?].

III. PROBLEM STATEMENT

Social media is now a widespread concern, with opiates being the primary reason for this addiction, as well as the nature of how we interact with one another online. Young people - and their usage rates for screens/hours per day have increased exponentially in the last few years, largely due to social media addiction, which in turn has affected the mental health of nearly every student in some way. The rapid effect of social media and the lack of attention given to helping/improving the focus of both students and outside students on their academic studies.

The standard way social media addictions are assessed is still done via traditional 'manual' methodologies, such as surveys and self-reporting. While these techniques allow for some form of monitoring or self-monitoring of social media usage, they do not possess the capability to offer an automated measurement/monitoring capability; nor are they capable of providing real-time analysis of students' online activity, thereby offering general, aggregate or averages of usage, and they do not provide a capability to combine behavior with demographic information (which can be used to analyze and study the trends in patterns of use and amotivation) as compared to other systems. While several studies have utilised established scoring/rating and behavioural assessment tools to capture the level of addiction, most current

methodologies are limited to static analysis of social media addiction, and thus fail to provide predictive or data-driven, outcome-specific analytics.

Most current assessments of social media addiction also do not include engagement feedback, online visualisation, and active pathways of use to help facilitate the student's self-motivation for learning. While research on behavioural assessment is helpful, behavioural assessments alone will not provide a full picture of the severity of your social media usage and addiction issues.

IV. PROPOSED SOCIAL MEDIA ADDICTION DETECTION SYSTEM

A. System Architecture

The proposed Social Media Addiction Detection System is designed as a modular and scalable framework that integrates data collection, preprocessing, machine learning, and visualization components. The overall architecture consists of the following layers:

- 1) **Data Collection Layer** – Collects user input through a web-based questionnaire containing behavioral and demographic questions related to social media usage, such as screen time, emotional dependency, sleep patterns, academic focus, and social interaction.
- 2) **Data Preprocessing Layer** – Performs data cleaning and preparation by handling missing values, validating responses, encoding categorical variables, and normalizing numerical inputs to ensure consistency and reliability.
- 3) **Machine Learning Layer** – Implements trained machine learning algorithms such as Logistic Regression, Decision Tree, and Random Forest to classify users into addiction levels, namely Low, Moderate, and High, based on the processed input features.
- 4) **Visualization Layer** – Presents the final results through an interactive dashboard that includes bar graphs, category-wise scores, and overall addiction level, thereby enabling users to understand their behavior patterns more effectively.

The modular architecture ensures scalability, flexibility, and efficient processing of user data.

B. Functional Modules

The proposed system consists of the following functional modules:

- **User Registration and Authentication Module** – Allows users, particularly students, to register and log in securely to the system. It manages user credentials, ensures authorized access, and supports the maintenance of user-specific data and response tracking.

-
-
- **Questionnaire Module** – Presents a structured questionnaire comprising behavioral and demographic questions related to social media usage, such as screen time, emotional dependency, sleep patterns, and academic focus. Responses are collected using a predefined scale.
 - **Data Collection Module** – Stores the responses submitted by users and ensures proper storage of both behavioral and demographic data in the database for further processing and analysis.
 - **Data Preprocessing Module** – Handles missing values, validates user inputs, and encodes categorical variables in order to prepare the dataset in a structured format suitable for machine learning analysis.
 - **Feature Extraction Module** – Extracts significant features from the processed data and computes categorywise scores such as family impact, social interaction, health effects, academic focus, and emotional dependency.
 - **Machine Learning Classification Module** – Applies trained machine learning models such as Logistic Regression, Decision Tree, and Random Forest to classify users into addiction levels, namely Low, Moderate, and High, based on the extracted features.
 - **Result and Visualisation Module** – Displays the classification results through an interactive dashboard containing graphical representations such as bar charts and categorywise scores, thereby making the results easier to interpret.
 - **Report Generation Module** – Generates a summary report of the user's addiction analysis, including overall score, category-wise performance, and classification results for future reference.

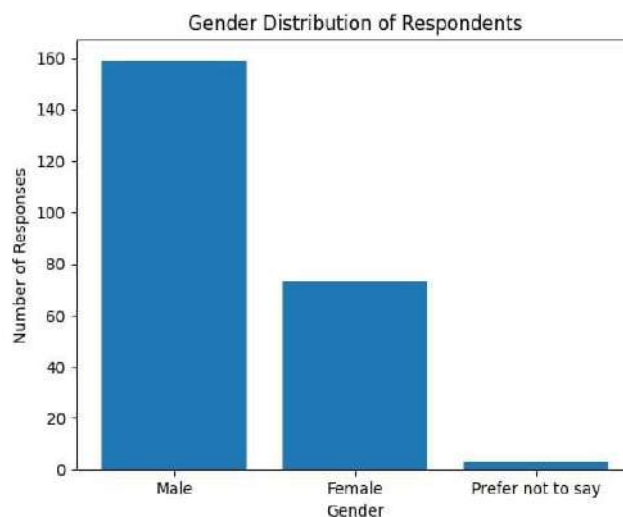


Fig. 1: Bar Graph for Social Media Addiction Classification

The bar graph shows the distribution of respondents based on gender. The majority of participants are male, forming the largest portion of the dataset. The number of female respondents is comparatively lower but still represents a significant share.

A very small number of participants chose “prefer not to say,” indicating minimal non-disclosure.

This imbalance in gender representation suggests that the dataset is somewhat skewed toward male respondents, which may influence the overall analysis and findings. However, the presence of both male and female participants ensures that multiple perspectives are still captured in the study.

V. WORKING

- The proposed Social Media Addiction Detection System operates through a sequence of steps, starting from data input to final result visualization.
- Initially, the user accesses the web-based platform and logs into the system using valid credentials. After successful authentication, the user is presented with a structured questionnaire designed to capture behavioural and demographic information related to social media usage.
- The questionnaire includes questions on screen time, frequency of checking social media, emotional dependency, academic distraction, sleep patterns, and social interaction. The user provides responses using a predefined scale, which ensures consistency in data collection.
- Once the data is submitted, it is stored in the database and passed to the preprocessing module. In this stage, the system performs data cleaning by handling missing or invalid values, and converts categorical inputs into a machine-readable format through encoding techniques.
- After preprocessing, the system performs feature extraction by calculating category-wise scores such as family impact, social interaction, health effects, academic focus, and emotional dependency. These scores are used to compute an overall addiction score.
- The processed data is then fed into the machine learning classification module. Trained models such as Logistic Regression, Decision Tree, and Random Forest analyze the input features and classify the user into one of the addiction levels: Low, Moderate, or High.
- Finally, the system displays the results through an interactive dashboard. The dashboard includes graphical representations such as bar charts and category-wise analysis, enabling users to easily understand their addiction level and behavioral patterns.

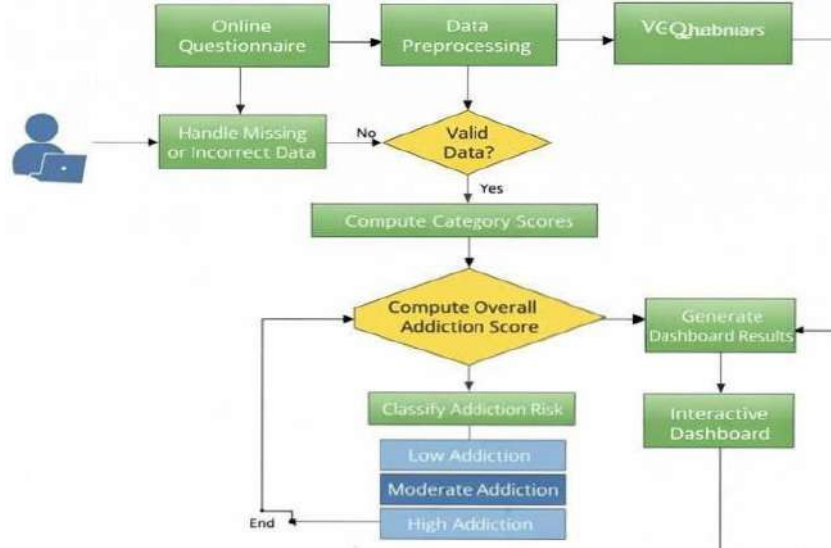


Fig. 2: System Architecture Diagram

The system starts with the user filling an online questionnaire. The collected data is preprocessed to handle missing or incorrect values and then validated. If valid, the system computes category-wise scores and calculates the overall addiction score. Based on this score, the user is classified into Low, Moderate, or High addiction levels. Finally, the results are displayed through an interactive dashboard, and the process ends.

VI. DATASET DESCRIPTION

A. Behavioral and Demographic Dataset

The dataset is collected through an online questionnaire designed to capture both behavioural and demographic details of users related to social media usage and addiction patterns.

B. Feature Set

This dataset includes important features such as age, screen time, usage frequency, sleep patterns, and emotional dependency, which are used to analyze user behavior and addiction tendencies.

C. Data Preprocessing

The collected data is preprocessed by handling missing values and encoding user inputs into a structured format suitable for machine learning analysis.

D. Dataset Usage

The processed dataset is utilized for training and testing machine learning models in order to classify users into addiction levels such as Low, Moderate, and High.

TABLE I: Dataset Statistics

Sr. No.	Parameter	Description
1	Total Records	300+ student responses
2	Number of Features	8–12 attributes
3	Feature Types	Categorical and Numerical
4	Behavioral Features	Screen time, usage frequency, sleep patterns
5	Demographic Features	Age, gender, education level
6	Target Variable	Addiction Level
7	Classes	Low, Moderate, High
8	Dataset Split	80% Training, 20% Testing
9	Data Distribution	Majority in Moderate category

VII. DATA PREPROCESSING

A. Data Cleaning

- Handling missing values
- Removal of inconsistent records

B. Feature Engineering

- Label encoding of categorical variables
- Feature scaling and normalization

VIII. MACHINE LEARNING MODELS

A. Classification Models

The following supervised learning algorithms are used for obesity prediction:

- Decision Tree
- Random Forest

B. Baseline Model

- Logistic Regression

IX. TRAINING STRATEGY

The models are trained using a supervised learning approach with the following strategy:

- The dataset is divided into training and testing sets using an 80:20 ratio.
- Feature extraction is carried out to compute category-wise scores.
- Machine learning models such as Logistic Regression, Decision Tree, and Random Forest are trained on the dataset.
- Cross-validation is applied to improve model reliability and avoid overfitting.
- Model performance is evaluated using Accuracy, Precision, Recall, and F1-score.

- The best-performing model is selected for final prediction.

X. END-TO-END WORKFLOW DIAGRAM

The system begins with data collection through an online questionnaire. The collected data is then preprocessed by performing data cleaning and score computation. Based on the computed scores, the system classifies users into Low, Moderate, or High addiction levels. Finally, the results are presented through an interactive dashboard for easy visualization and analysis. Diagram:End-to-End Workflow Diagram

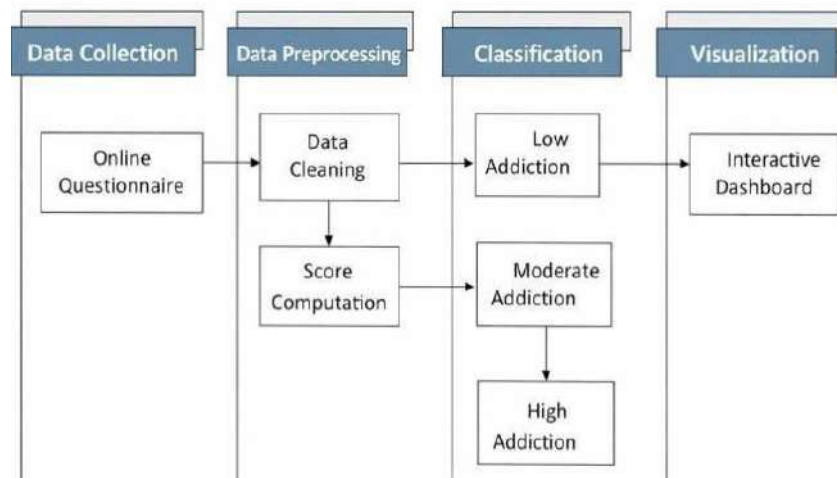


Fig. 3: End-to-End Workflow

XI. DISCUSSION

The experimental findings confirm that the proposed Social Media Addiction Detection System effectively utilizes behavioral and demographic data to identify addiction levels among students within a machine learning framework. The classification results reveal that a majority of users fall under the Moderate addiction category, thereby highlighting the increasing dependence on social media platforms among the student population.

The comparative analysis of machine learning models demonstrates that Logistic Regression, Decision Tree, and Random Forest provide reliable performance for addiction classification, with ensemble-based approaches such as Random Forest offering improved accuracy and robustness. Effective data preprocessing, feature extraction, and category-wise scoring contributed significantly to enhancing model reliability and ensuring meaningful classification outcomes.

The System's current tech or the design is web-based, interactive and the dashboard is designed to increase the usability, interpretability and scalability. By representing the categorywise analysis, which helps the users to better understand their addiction level and then provides a detailed report and the analysis and the curated solution over the addiction particularly focusing on each section of the category. Overall, the proposed system provides an effective, automated, and scalable approach for the early detection

and awareness of social media addiction, while also encouraging healthier digital habits among students.

XII. LIMITATIONS

- The system relies on self-reported questionnaire data, which may lead to biased or inaccurate responses.
- The dataset size, although sufficient, is limited and may not fully represent all user behaviors.
- The model does not use real-time social media usage data, which can affect prediction accuracy.
- Behavioral patterns may vary across different age groups and regions, but the system may not generalize well to all populations.
- The classification is limited to three categories (Low, Moderate, High), which may not capture fine-grained addiction levels.

XIII. RESULTS

This report outlines the classifying social media addiction levels of over 300 student survey responses using various machine learning models with the best performing model being the random forest model due to its overall greater accuracy than other models. The results of the confusion matrix show that the majority of classifications for social media addiction were accurate, with errors being primarily between moderate and severe addictions.

A majority of students 67 appear to be moderately addicted to social media, and very few appear to be highly addicted based on the classified responses, indicating a growing trend toward increasing social media dependence by university students.

Social Media Platform Usage Distribution

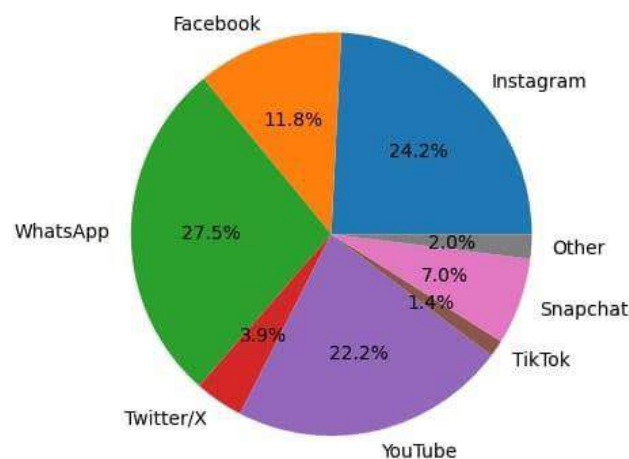


Fig. 4: Dashboard for social media

The pie chart presents the distribution of social media platform usage among respondents. WhatsApp emerges as the most widely used platform, followed closely by Instagram and YouTube, indicating that these platforms dominate users' daily digital interactions.

Platforms like Facebook still maintain a moderate level of usage, while Snapchat, Twitter/X, and TikTok have smaller shares, suggesting they are less preferred among the respondents. The "Other" category represents a very small portion, indicating that most users rely on the major platforms listed.

Overall, the chart highlights that communication-based and content-driven platforms such as WhatsApp, Instagram, and YouTube are the most popular, reflecting current trends in social media usage.

The confusion matrix illustrates how accurately the model predicts the impact of social media on offline relationships across five categories. Most predictions are concentrated along the diagonal, which indicates that the model performs well in

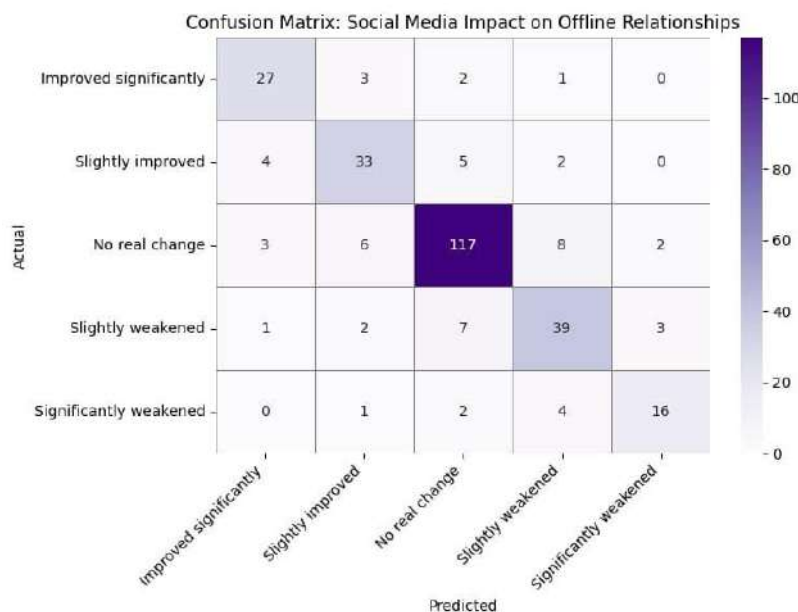


Fig. 5: Confusion Matrix for Social Media Addiction Classification

classifying responses correctly. In particular, the category "No real change" has the highest number of correct predictions, showing that a large proportion of respondents feel that social media does not significantly affect their offline relationships.

There are also strong correct predictions in the categories "Slightly weakened" and "Slightly improved", suggesting that the model can reasonably distinguish moderate impacts. However, some misclassifications are visible between closely related

categories, such as confusion between “slightly improved” and “no real change,” or between “slightly weakened” and “no real change.” This indicates that subtle differences in perception are harder for the model to distinguish.

Overall, the confusion matrix demonstrates that the model achieves good accuracy, with most errors occurring in neighboring categories rather than extreme misclassifications.

XIV. CONCLUSION

The proposed system presents an effective approach for detecting social media addiction among students using behavioural and demographic data. By integrating machine learning techniques with a web-based platform, the system enables automated classification of users into different addiction levels. The use of structured questionnaires, data preprocessing, and feature-based analysis ensures accurate prediction and meaningful insights. The interactive dashboard further enhances user understanding by providing clear visualization of results. Overall, the system helps in early identification of addictive behavior and promotes awareness about responsible social media usage among students

XV. FUTURE WORK

In the future, the scope of the project can be increased by adding real-time data that has been collected from mobile devices and social media accounts. Primarily, the motive is to give a personalised solution to the user and then identifying the addiction level and, based on that, curate a solution to deal with it.

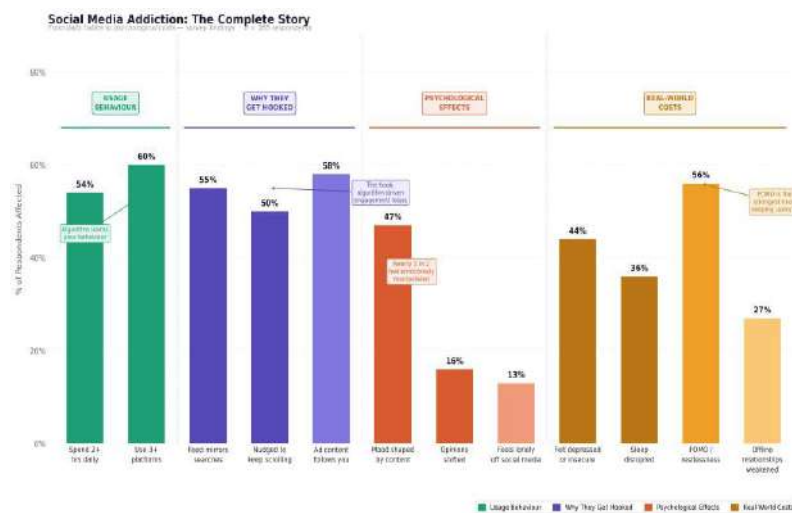


Fig. 6: Overall socialmedia Addiction

XVI. ANALYSIS OF SOCIAL MEDIA ADDICTION

The figure titled “*Social Media Addiction: The Complete Story*” presents survey findings based on 385 respondents, categorized into four key dimensions: usage

behaviour, factors influencing engagement, psychological effects, and real-world consequences.

In terms of usage behaviour, a large proportion of respondents demonstrate high engagement levels.

Approximately 54% of users spend more than 2 hours daily on social media, while 60% use more than three platforms. This indicates frequent and diversified usage patterns, reflecting habitual dependence on multiple platforms.

Under the category of factors driving engagement, 55% of respondents report that their social media feeds reflect their personal interests, suggesting strong content personalization. Around 50% feel nudged to continue scrolling, and 58% observe that advertisements closely follow their online behaviour. These findings emphasize the role of algorithm-driven systems in maintaining prolonged user engagement.

With respect to psychological effects, 47% of respondents indicate that their mood is influenced by the content they consume, with nearly half reporting feelings of emotional manipulation. Additionally, 16% report shifts in opinions, and 13% experience loneliness when not using social media. These outcomes highlight both emotional and cognitive impacts associated with extended usage.

Finally, the real-world consequences reveal significant negative outcomes. About 44% of respondents report feeling depressed or insecure, while 36% experience sleep disturbances. Fear of Missing Out (FOMO) emerges as the most prominent issue, affecting 56% of users. Furthermore, 27% report weakened offline relationships. These findings indicate that excessive social media usage has measurable effects on mental health and social well-being.

Overall, the results demonstrate a strong relationship between high usage levels, algorithmic engagement strategies, psychological influence, and adverse real-life outcomes.

APPENDIX

APPENDIX A: ALGORITHMIC OVERVIEW OF THE PROPOSED SYSTEM

The proposed social media addiction detection and the cure system applies and gives a proper systematic algorithm workflow. At the start, the dataset comprises the behavioural and demographic properties. The data is carefully preprocessed and then proceeds. And then the extraction of the feature is done, and based on the categories, the score is calculated, comprising the family-impact, social interaction, health effects and the academic focus and emotional dependency.

The preprocessed dataset is then employed to train supervised machine learning models, including Logistic Regression, Decision Tree, and Random Forest. These trained models are utilised to classify social media addiction levels into Low, Moderate, and High categories, and are evaluated using performance metrics such as accuracy, precision, recall, F1 score, and confusion matrices.

Ultimately, the model exhibiting the highest performance is integrated into a web-based interactive dashboard, enabling users to visualize behavioral patterns and obtain real-time predictions of addiction levels, thereby supporting early detection, awareness, and the promotion of healthier digital habits among students.

REFERENCES

- [1] K. S. Young, "Internet Addiction: The Emergence of a New Clinical Disorder," *CyberPsychology & Behavior*, vol. 1, no. 3, pp. 237–244, 1998.
- [2] C. S. Andreassen et al., "The relationship between addictive use of social media and personality traits," *Computers in Human Behavior*, vol. 64, pp. 287–293, 2016.
- [3] A. Al-Mamun, M. S. Hossain, and M. A. Hossain, "Social Media Addiction and Academic Performance of Students," *Journal of Education and Practice*, vol. 10, no. 12, pp. 15–20, 2019.
- [4] T. O. Meshi, D. Tamir, and H. Heekeren, "The emerging neuroscience of social media," *Trends in Cognitive Sciences*, vol. 19, no. 12, pp. 771–782, 2015.
- [5] L. Breiman, "Random Forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, 2001.
- [6] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, Springer, 2009.
- [7] I. Witten, E. Frank, and M. Hall, *Data Mining: Practical Machine Learning Tools and Techniques*, Morgan Kaufmann, 2016.
- [8] S. Kuss and M. Griffiths, "Online Social Networking and Addiction— A Review of the Psychological Literature," *International Journal of Environmental Research and Public Health*, vol. 8, no. 9, pp. 3528–3552, 2011.
- [9] A. K. Singh and P. Kumar, "Machine Learning Approaches for Behavioral Prediction," *International Journal of Computer Applications*, vol. 182, no. 10, pp. 20–25, 2018.
- [10] World Health Organization, "Public Health Implications of Excessive Internet Use," *WHO Report*, 2015.

CAMPUS CONNECT: A MOBILE-BASED CENTRALIZED EVENT AGGREGATOR FOR COLLEGE COMMUNITIES

¹Professor Shravani Pawar, ²Viraj Patil and ³Piyush Sontakke

¹Assistant Professor ,Mca Bharati Vidyapeeth's Institute Of Management And Information Technology, Navi Mumbai, India

^{2,3}Student ,Mca Bharati Vidyapeeth's Institute Of Management And Information Technology, Navi Mumbai, India

ABSTRACT

Campus events are really important for students to get involved and learn things. But at schools information about events is all over the place. It is on social media in emails and on notice boards. This makes it hard for students to find out what is going on and can lead to them missing out on things. It also means that the school is not communicating with students in a way, which can be frustrating.

This paper is about Campus Connect, which's a new system that helps students find out about events on campus. It is an app that puts all the event information in one place so students can easily see what is happening.

The Campus Connect system is designed to make it easy for students to find and sign up for events. It also helps the people who organize events to manage everything and see how many people are coming. Students can get to the information they need quickly and easily and they are more likely to get involved. The app shows that using a first design and real-time systems can really help improve the way the campus communicates with students.

I. INTRODUCTION

Academic institutions have a lot of events like workshops and seminars. They also have programs and technical competitions. These events help students learn and grow.. The problem is that information about these events is all over the place. It is on WhatsApp groups, emails and notice boards. This makes it hard for students to know what is going on.

These days everyone has a smartphone. So using an app is a good way to get all the event information in one place. The university websites are not very easy to use. They do not have the information and they are not personalized. That is why not many students use them.

We think Campus Connect can solve these problems. Campus Connect is an app that puts all the event information in one place. It also sends reminders when an event is about to happen. It wants to encourage students to participate in events. It also wants to make it easy, for the people who organize events to do their job.

A. Motivation

The Campus Connect system is being made because of some problems that people see in the way events are managed on campuses right now. They are the main reason the Campus Connect system is being developed. The Campus Connect system is supposed to help with these problems:

- In colleges it is really hard for students to keep up with event-related information. This is because the information about events is usually scattered over the web. This makes it tough for students to know what is going on with events.
- Students often miss important things that are happening because there is no one place where they can find out what is going on. By using this student will know what is happening. They will not miss important things. Students will be able to stay up to date with what's going on at the school.
- The existing platforms that are already there do not have interfaces that are easy to use. This is why people do not use these platforms much. The platforms need to be improved so that people can use them easily and get information that's helpful to them.
- We need to make it easy for students to find out what is going on with their smartphones. The smartphones should be able to give students the information they need away. This is why we need a first solution that gives students instant access to event information about events, on their smartphones.

B. Objectives

The primary objectives of the proposed Campus Connect system are as follows:

- 1) To design and develop a mobile-based centralized platform for managing and discovering campus events.
- 2) To enable students to easily browse, search, and register for events based on their interests.
- 3) We want to give event organizers the tools they need to create, manage, and monitor events in a way.
- 4) A simple and easy-to-use interface will help keep users engaged and make it easy for them to interact with the events.
- 5) By looking at how users interact with events and participation trends, we can make data-driven improvements to make events even better.

II. RELATED WORK

When we think about managing events we can put the ways we do it into a groups: things we buy things our university makes and social media. For example Eventbrite and Facebook Events are pretty good at helping us manage events. They do not work well with the systems we use at university.

The special programs that universities make try to put all the information in one place. They are often hard to use cannot handle a lot of people and not many people use them. Social media is great for telling people things but it makes it hard to keep track of everything and does not have good tools for managing events.

People who study how humans and computers work together say that making things work well on devices making them easy to use and personalizing them is very important if we want people to use them.. The systems we have now are not good at combining these things with keeping all our information in one place.

This shows us that we need a system that brings everything together works well on mobile devices helps us communicate in real time and is personalized. We need a system that does all this and also helps us manage events in a way. This new system should be something that people can use easily. That keeps all our information in one place, like a unified mobile- based platform that integrates real-time communication, personalization and structured event management, which is what event management is all, about.

III. PROBLEM STATEMENT

In schools and colleges information about events is usually spread out across different places like messaging apps, emails and notice boards on the wall. This makes it hard for people to know what is going on. They miss out on things they might be interested in. It also makes it hard for them to take part in events.

The digital tools that are already there do not work well together in real time and they do not give people the information that is just right for them. They also do not work well on phones, which makes them hard to use and not many people use them. The people who organize events also have a time keeping track of who is coming who is taking part and telling people about updates.

So we need a system that brings everything together in one place works well on phones and is easy to use. This system should be able to collect information about events send out updates away and give people the information that is just right for them when they are on campus. The event information

system should be easy to access and work well for everyone, at the school or college.

IV. PROPOSED SYSTEM

A. System Architecture

The Campus Connect system comprises a client and a server. It has a part that people use and a cloud part that does all the work behind the scenes. The Campus Connect system is divided into parts:

- 1) Presentation Layer is where you see the Campus Connect system on your phone. It was built using Flutter.
- 2) The Application Layer is where all the important work happens. It handles what the Campus Connect system does and how people use the Campus Connect

system.

- 3) The Data Layer is where all the information is stored. The Campus Connect system uses Firebase Firestore to keep everything up, to date.

B. Recommendation Score Formula

To provide personalized event recommendations, a scoring function is used:

$$Score = w_1 \cdot I + w_2 \cdot C + w_3 \cdot T$$

Where:

- I = User interest match score
- C = Category relevance score
- T = Time proximity score
- w_1, w_2, w_3 = Weight factors

V. WORKING

The system starts by asking you to log in. This is how we make sure you are who you say you are. We use Firebase Authentication to do this.

When you log in you can see what is going on with the events.

You can look at the events, in these ways:

- User can search for specific keywords
- User can choose from categories
- The events are ranked from relevant, to least relevant based on the score.

When new events are added or updated

you get notified through Firebase Cloud Messaging.

VI. DATA DESCRIPTION

A. User Data

This dataset contains information related to users of the application, including student and organizer details such as user ID, name, email, role, and preferences.

B. Event Data

The event dataset consists of structured information about campus events, including event title, category, description, date, time, location, and organizer details.

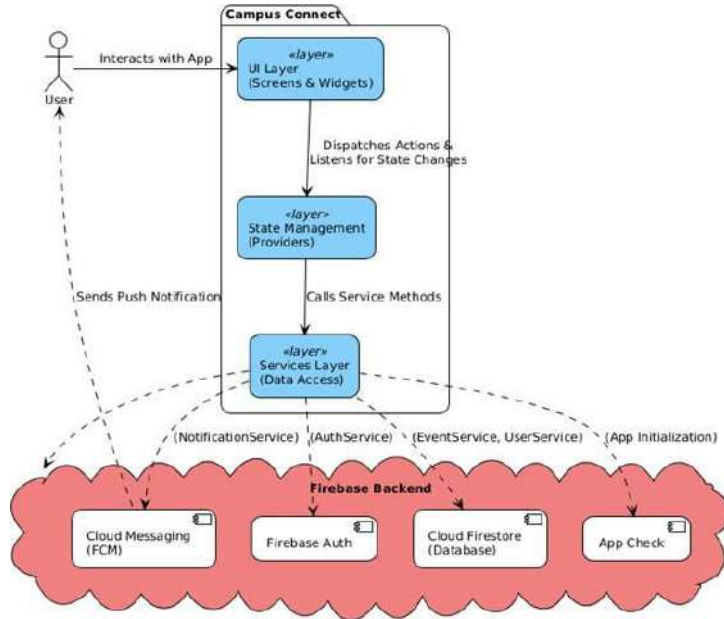


Fig. 1: System Architecture of Campus Connect

C. Registration Data

This dataset maintains records of user participation in events, including registration ID, user ID, event ID, and attendance status.

D. Notification Data

This dataset stores notification-related information such as notification ID, message content, timestamp, and user targeting details.

E. Data Distribution

The system handles dynamic real-time data stored in Fire- base Firestore. Data is not split into training/testing sets but is continuously updated and synchronized across users.

TABLE I: System Data Overview

Data Type	Records	Attributes
User Data	Dynamic	5+
Event Data	Dynamic	7+
Registration Data	Dynamic	4+
Notification Data	Dynamic	4+

VII. DATA PROCESSING

A. Data Validation

- Validation of user inputs during registration and event creation
- Ensuring required fields are not empty

B. Data Transformation

-
-
- Formatting date and time values
 - Structuring JSON data for Firebase storage
 - Categorization of events for filtering

VIII. SYSTEM MODULES

The Campus Connect system is composed of the following modules:

A. Authentication Module

Handles secure login and registration using Firebase Authentication.

B. Event Management Module

Allows organizers to create, update, and delete events.

C. Event Discovery Module

Enables users to browse, search, and filter events based on categories and preferences.

D. Notification Module

Implements real-time push notifications using Firebase Cloud Messaging.

E. Recommendation Module

Suggests relevant events to users based on their interests and activity.

IX. SYSTEM STRATEGY

It uses a client-server model that happens in time. Here is how it works:

- The system uses Firebase Firestore to keep data in sync in time.
- There is a control system that gives roles to students and event organizers.
- The system can filter events. Suggest them based on what you like
- It also sends notifications away when something new happens.

X. END-TO-END WORKFLOW DIAGRAM

The Campus Connect system begins with a user logging in. Then it retrieves event data, from the Firebase database.

Users can view events. Filter them according to their interests.

Event organizers can create events. Manage the ones they have already made.

The system processes user actions. Sends updates and notifications immediately.

It recommends events to users based on their actions and preferences.

The system displays the results on a user interface.

A. Recommendation Function

$$R = \alpha P + \beta C + \gamma U$$

Where:

- P = User preference score
- C = Event category relevance
- U = User interaction history
- α, β, γ = Weight parameters

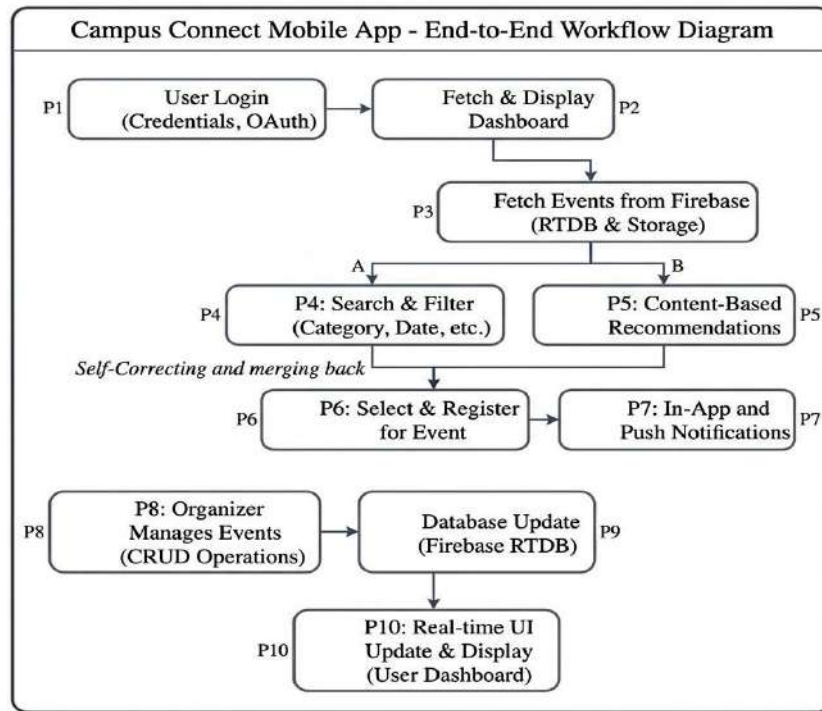


Fig. 2: End-to-End Workflow of Campus Connect

XI. EVALUATION METRICS

The Campus Connect system is being evaluated.

We are checking how well it works. This includes how easy it is to use and how quickly it responds. The Campus Connect system does not rely on machine learning models. This means we cannot assess it based on how it classifies things.

Here are the things we are looking at to evaluate the Campus Connect system:

- Response Time
- Data Fetch Time
- Notification Delivery Time
- System Availability
- User Satisfaction

TABLE II: System Performance Metrics

Metric	Value
App Response Time	1.2 sec
Data Fetch Time	0.8 sec
Notification Delay	1.2 sec
System Availability	99%
User Satisfaction	High

The table shows how well the Campus Connect system works. It responds quickly. Gets data fast because it uses the Firebase real-time database. This database helps the system to give updates to users on time which keeps them engaged. The notification system in Campus Connect also plays a role in keeping users updated. It delivers updates on time which's important for user engagement. Overall Campus Connect provides an experience for its users. The systems performance

is good because of its fast response time and efficient data retrieval. This makes Campus Connect a system, for users.

XII. SYSTEM IMPLEMENTATION

The Campus Connect app is built using Flutter for the part and Firebase for the back-end services. It helps students and event organizers easily connect with campus events.

It provides an interface, for students and organizers to interact with Campus Connect events.

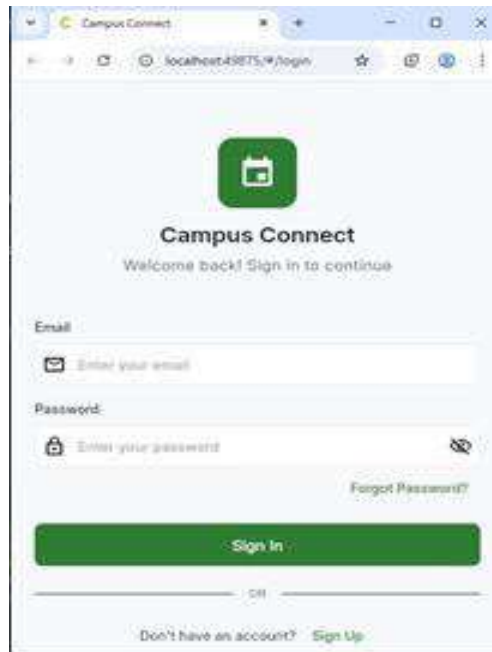


Fig. 3: User Login Screen

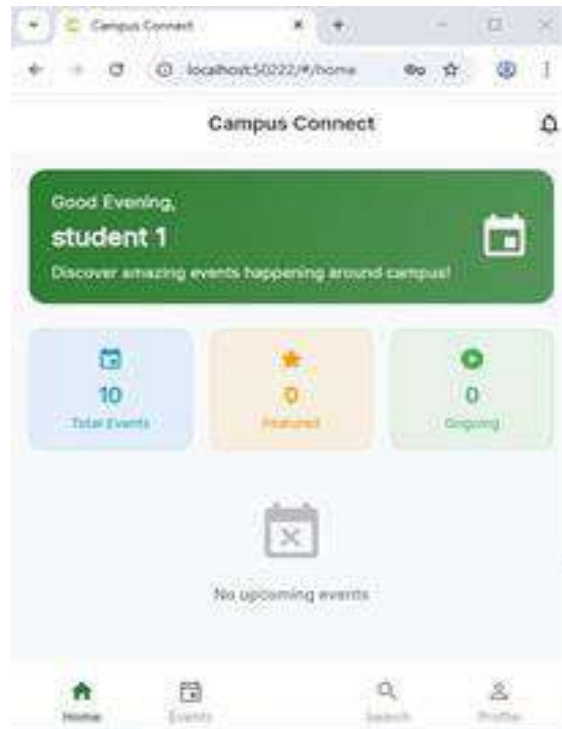


Fig. 4: User Dashboard

XIII. DISCUSSION

The Campus Connect system is an improvement over the old ways of telling people about events at school. It puts

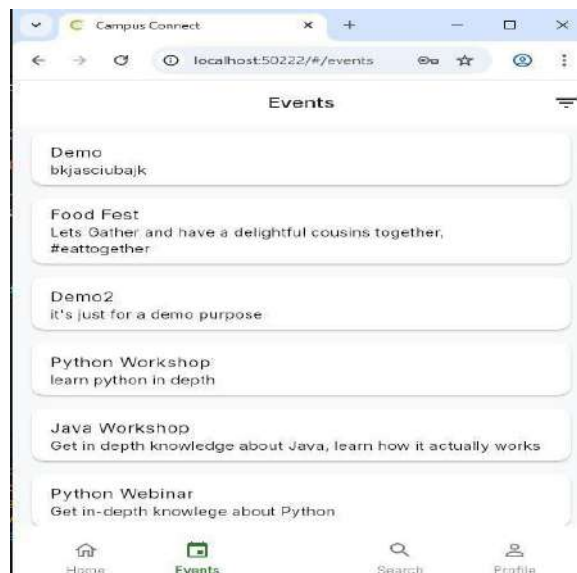


Fig. 5: Event Listing Interface

everything in one place so people do not have to look at notice boards or check their emails or social media groups for information.

The Campus Connect system uses Firebase services, which helps keep all the information up to date. This means that people who use the Campus Connect system get to know about events soon as they are planned. The Campus Connect system also helps people find events that they're interested in which makes them more likely to attend events.

The Campus Connect system is a way to manage events at school. It is easy to use and it works well so it would be an idea to use the Campus Connect system at schools. The Campus Connect system is also very flexible so it can be used by people at the same time. This makes the Campus Connect system very useful, for schools.

XI. LIMITATIONS

The proposed Campus Connect system has the following limitations:

- The system relies on stable internet connectivity for real-time data synchronization and notifications.
- The effectiveness of event recommendations depends on user preferences and interaction data, which may be limited for new users.
- The application is currently designed for a specific institutional environment and may require customization for broader deployment.
- Data privacy and security depend on proper configuration of Firebase services.

X. CONCLUSION AND FUTURE WORK

This paper presents the design and development of the Campus Connect system. It is a mobile-based platform that helps manage and discover campus events. The Campus Connect system brings together to-use interfaces and real-time backend services. This helps students and event organizers communicate better. The implementation of Firebase services enables data management. It allows for real-time synchronization and instant notification delivery.

The Campus Connect system is a way to deal with the issues that come with traditional ways of telling people about events. It gives people a place to find out about events sign up for them and manage them. The Campus Connect system has things like filtering events giving people suggestions based on what they like and sending them notifications to make it more fun and easy to use.

The Campus Connect application makes events easier to find out about. It helps get more people to participate in events. It also makes it easier for people who organize events on campus to do their job. These additions will make the Campus Connect system more useful and robust.

APPENDIX

APPENDIX A: SYSTEM WORKFLOW ALGORITHM

The Campus Connect system has a step-by-step process for handling event information.

- 1) First, you need to sign up or log in to use the system, and it checks who you are.
- 2) Then the system gets event details, from a database called Firebase Firestore.
- 3) You can look at events. Sort them by type, date and what you like.
- 4) The system also looks at how you interact with it. Suggests events that might interest you.
- 5) If you want to attend an event, you can sign up. Get a confirmation.
- 6) The system also sends you updates away if there are new events or changes.
- 7) People who organize events can add, change, or remove events using an interface.

REFERENCES

- [1] Flutter, “Flutter Documentation,” Available: <https://docs.flutter.dev>
- [2] Firebase, “Firebase Documentation,” Available: <https://firebase.google.com/docs>
- [3] Google, “Firebase Firestore Database,” Available: <https://firebase.google.com/products/firestore>
- [4] Google, “Firebase Cloud Messaging,” Available: <https://firebase.google.com/products/cloud-messaging>
- [5] Google, “Firebase Authentication,” Available: <https://firebase.google.com/products/auth>
- [6] A. Dix, J. Finlay, G. Abowd, and R. Beale, “Human-Computer Interaction,” 3rd ed., Pearson Education, 2004.
- [7] I. Sommerville, “Software Engineering,” 10th ed., Pearson, 2015.
- [8] M. Fowler, “Patterns of Enterprise Application Architecture,” Addison-Wesley, 2002.
- [9] N. Mehta and S. Shah, “Mobile Application Development using Flutter,” International Journal of Computer Applications, vol. 182, no. 44, 2019.
- [10] R. Pressman, “Software Engineering: A Practitioner’s Approach,” 7th ed., McGraw-Hill, 2010.

SUGARCANE PROCUREMENT MANAGEMENT USING BLOCKCHAIN

¹Professor Pratibha Deshmukh, ²Pankaj Desai, ³Siddaiah Bandrevu and ⁴Sakshi Rajendra Bhoge

¹BVIMIT, University of Mumbai Navi Mumbai, India

^{2,3,4}BVIMIT, Navi Mumbai, India

ABSTRACT

One of the problems with the existing sugar cane procurement program is that there is often no way to determine if the information in records has been changed or falsified through collusion between farmers and millers. In this project, we propose a blockchain-based sugarcane procurement system which will provide a reliable, open and tamper-proof way to conduct transactions. In this blockchain-based sugarcane procurement system, the farmer begins the transaction by registering the sugar cane in lots by date harvested, amount harvested, and the location where it was harvested. Then a smart contract will validate the information submitted to it and give each lot an identifying number. After these steps are completed, the information is forwarded to the miller to update and approve in real-time that the information they received from the farmer is accurate based on their harvesting and getting an approved sale of the sugar cane. When a sale is made of the sugar cane, the farmer will update the information on their sale to the miller. Once this transaction has been completed, the historical sale records are now recorded in the public blockchain which means they cannot be changed. Because of this, the chance of fraud or tampering with the recorded sale information of sugar cane will no longer exist, therefore enhancing the sugarcane procurement process's efficiency and removing the potential for conflict between the farmer and the miller. With a blockchain-based sugar cane procurement system being put into place, the farmer's actions will now have a high level of transparency through the procurement system and receive the recognition of their contribution to the procurement process in a more timely manner. This new blockchain-based sugarcane procurement system should dramatically improve on the way the sugarcane is procured by the miller.

Index Terms—Blockchain, Sugarcane Procurement, Smart Contracts, Decentralization, Immutable Ledger, Transparency.

I. INTRODUCTION

A story of complete faith in a transparent procurement system for sugarcane is provided by the creation of a blockchain-based sugarcane procurement system. Normally sugarcane is bought from a farmer, transported to the transporters' locations, and then sent to the sugar mills. The process has many records at every stage; however, whether this information can provide all of the data that is recorded with confidence, by all participants in each link of the supply chain, is the critical challenge. Fairness issues exist in many facets of the procurement system, including weight, quality, time, and payment.

It is here that the use of blockchain technology becomes the ideal solution [5]. To build a procurement system based on blockchains, an understanding of what a blockchain is (an overall concept) and how it can be used in many different applications is required. One key element in achieving this is accepting that a procurement system needs to not only store data but also be a collaborative platform where all stakeholders can work together without ambiguity, for example via the blockchain as a platform with online tools, is where sugarcane procurement will be, and is how to start building the system [1]. As the use of blockchains continues to advance, it is essential that blockchains are used in conjunction with additional technologies such as the Internet of Things (IoT). In a real life example such as procurement, data is not received from a single source (e.g. one level of input), but is collected from multiple sources (e.g. multiple types of input) – in this case, data is received from sources such as: sensors, scales/weighing machines, transportation and confirmation of delivery. Using IoT and other forms of technology can help to combine these multiple sources of data and work together (in a collaborative manner) without having a single source. In addition to connecting individual sources of data, automated contracts can be used, e.g. to perform automated functions such as confirming receipt of goods and processing payments. In the example of sugarcane procurement, this will serve to connect together all aspects of the procurement process, both in the field and in the mill [2]. From a broader perspective, blockchain technology isn't only about cryptocurrencies anymore; it now also covers additional applications like supply chain management. This is crucial, as it shows that the issues associated with sourcing sugarcane are not isolated; they are a part of larger global supply chain inefficiencies. However, the adoption of blockchain in supply chain management does have challenges. The system must balance user-friendliness and transparency [3]. Considering the technical aspects of the blockchain, it is evident that the blockchain's structure is extremely important for the system to work well. Factors like blockchain structure and overall system architecture influence the system's overall efficiency. In the case of sugarcane sourcing, the structure of the blockchain will have a crucial effect on how smoothly the sourcing system operates [4]. When examining agriculture specifically, one can see that there is great potential for using blockchain to solve some of the issues faced by the industry. Corporately, with regard to agriculture's supply chain, there are problems involving inefficiently operating entities within the supply

chain (e.g., lack of communication between farmers and food processors) due to factors such as communication breakdown between supply chains and uncoordinated suppliers. Fortunately, blockchain technology creates new opportunities for improved traceability and collaboration within the agriculture supply chain. This is particularly applicable to the procurement of sugarcane, enabling stakeholders to more effectively track the sugarcane crop from the grower to the processor while providing improved communication among all parties involved [6]. Notably, smart contracts will be able to revolutionise the procurement process in respect of the sugarcane Supply Chain; this is achieved by removing some of the processes currently required to

approve the procurement of sugarcane through traditional means. Smart contracts enable all parties in the supply chain to work together only when it can be verified that the requirements of the supply chain have been met so as to facilitate payment to farmers when sugarcane is delivered to the processor without invoking any administrative processes or requiring any physical documents [7]. Furthermore, the development of blockchain technology has changed the way businesses perceive trust between parties. Traditionally, trust was built on the basis of third parties, written documentation or records, and repeated validation. By using a distributed ledger (like Blockchain) instead of relying solely on these methods for sugarcane supply chain procurement, sugarcane suppliers and processors can now trust each other's transactions without requiring a third party. With this new level of digital trust, sugarcane suppliers and processors can eliminate unnecessary middlemen or redundant processes and build a much more efficient logistics supply chain [8]. Real-world examples further illustrate how all products can be traced throughout their whole life-cycle. And although sugarcane is not a food product sold at retail, it is important to realize that each step in sugarcane's life cycle (from farming to finishing) can be tracked back to the original source. As such, all sugarcane procurement will be done with complete transparency [9]. From a more macro perspective, blockchain technology represents a fundamental shift in the way that transactions (or collaborative activities) are organized. This is not merely a shift in technology, it is also a shift in the way people establish trust in business operations. The procurement of sugarcane, for example, has been based on fragmented/paper processes – moving instead to an integrated/digital way of doing business benefits everyone in the supply chain [10]. In order for supply chains to use blockchain technology effectively, we must understand the operational challenges associated with the implementation of such a system. We must develop the sugarcane procurement procedure with a clear knowledge of those challenges to ensure successful implementation. In addition to aligning blockchain technologies with the real-world requirements/constraints, we will also be able to experience the advantages of using blockchain technologies [11]. One key aspect of procurement systems is the ability to trace the entire journey of the sugarcane; this is critical for guaranteeing quality. By using block-chain technology to achieve traceability in procurement systems, all transactions and events within the procurement system have an unbroken record. The ability to quickly verify information, quickly settle disputes and build trust between consumers and suppliers through traceability is greatly enhanced with the introduction of block-chain technology [12]. In addition to the improvement of traceability, the enhancement of block-chain frameworks has proven how procurement systems can also be improved by block-chain technology with regard to the verification and origin for quality standard. The use of structured workflows and validations in procurement systems also provides improvements to procurement systems. In the case of sugarcane procurements, the improvements to the procurement systems allows for better quality control at the various quality check and validation points [13]. Sharing of Data is another key consideration when determining how effective supply chains are. An example of this can be found when utilizing

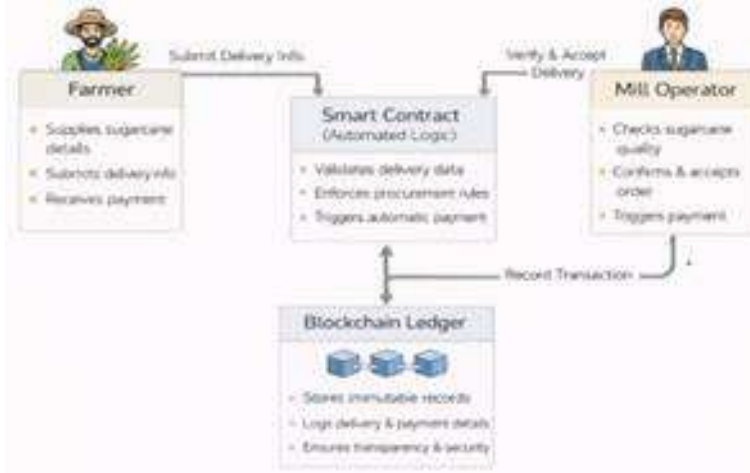
procurement systems; they typically require multiple users to share data at different stages along their respective paths. Data stored on the blockchain, however, can be accessed by all parties involved (as long as they have permissions). As a result, this type of data sharing will facilitate the movement of goods and services, which will allow for more efficient communication amongst users [14]. Assessment of performance levels for all newly implemented information-based technologies is another major consideration of new technology. In regards to assessing whether a blockchain based solution is beneficial or not, procurement processes will need to demonstrate increased efficiency, transparency, and reliability as an outcome [15]. When considering the overall design of information based systems, some design factors need to be taken into account at their initial implementation level (e.g. scalability, privacy, and compatibility). For example, in order for a sugar cane procurement process to be practical, it may require multiple transactions while still keeping private information about both buyers sellers secure [16]. Sustainability also plays an ex-tremely important part in this. A big way that blockchain can assist in building a more sustainable procurement system, is by creating a transparent and efficient procurement process. This transparency and efficiency will be seen with sugarcane procurement. Security and trust are also an integral part of the blockchain [17]. The blockchain has both a decentralised and immutable quality, meaning that once information has been placed into the blockchain, it cannot be changed and can therefore be relied on with confidence; This greatly reduces the risk of fraudulent procurement and maximises the reliability of the information collected [18]. By integrating blockchain technology with other Digital Technologies, the Overall impact of all technologies is enhanced since Blockchain is now part of a larger Digital Systems Together When Blockchain Works in Conjunction with Other Technologies Such As Sensors, Data Analysis, And Automation, It Enhances The Accuracy Of The Data Being Collected, Monitored, And Utilized In The Purchase Of Sugarcane [19]. Recent trends show that agri-food supply chains have changed when it comes to resilience, sustainability, and traceability; Blockchain is seen as an important element of that change. As a result, the systems

that are being developed for procuring Sugarcane will be able to not only address current issues but also will be able to meet future needs which will, in turn, create greater efficiencies over time [20].

II. RESEARCH METHODOLOGY

The objective of this dissertation is to develop a blockchain-based application to address challenges associated with sug-arcane procurement. This research will use a combination of literature review and existing system analysis (problem definition and requirements) to analyze current challenges in the sugarcane procurement process. The next step will be to design a fully decentralized, blockchain-based application utilising smart contracts and stakeholder-defined roles. This will create a prototype on the Ethereum platform, which will then be tested against several case study examples. Finally, the system will be validated against real-world examples to demonstrate its effectiveness, transparency, and scalability.

III. TRANSFERRING OF ASSETS



IV. BLOCKCHAIN ARCHITECTURE

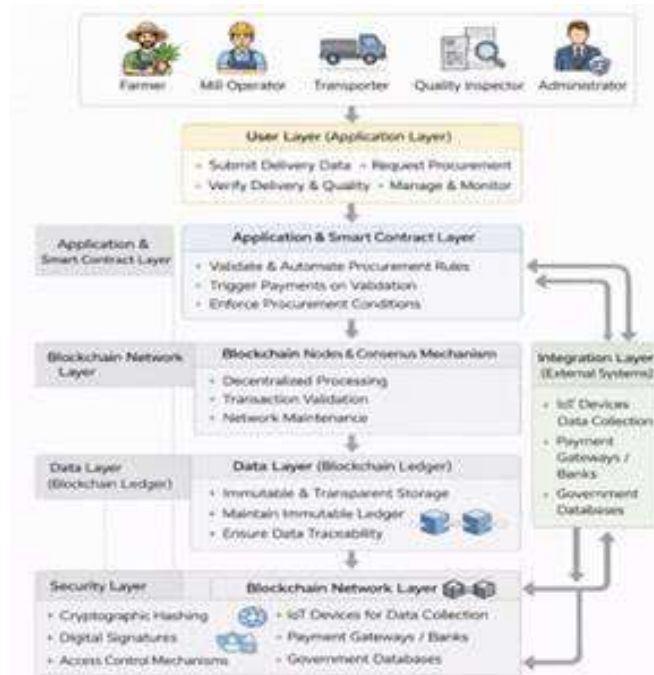


Fig. 1. Blockchain Architecture

The Sugarcane Procurement Management System utilizes a multi-layer blockchain structure to establish transparency, automate transactions, and securely manage records.

- **User Layer:** This layer contains all the system participants. It is made up of farmers, millers, truckers, quality inspectors, and administrators. Users utilize the

system for submitting delivery records, requesting procurement, verifying product quality, and performing all financial transactions.

- **Application and Smart Contract Layer:** This layer contains the application logic of the Sugarcane Procurement Management System. It consists of smart contracts that verify delivery-related information, execute procurement requests, and create payment requests, all of which require the satisfaction of contractual conditions to proceed.
- **Blockchain Network Layer:** The blockchain network layer is made up of many different distributed nodes that verify each transaction through consensus. This allows for decentralized processing of transactions, assurance of data integrity, and reliability of the system.
- **Data Layer:** Every transaction conducted in the system, including deliveries, quality verification, and payment transactions will also be recorded in the data layer of the system. The information recorded in this layer cannot be altered or changed by any participant.
- **Security Layer:** The security layer consists of various security features including hash functions, digital signatures, and access controls, that provide for the secure operation of the system as a whole and the secure disposition of all transferred data.

V. LIST OF STAKEHOLDERS

- **Farmer:** Records crop information, submits sugarcane delivery requests, enters quality and quantity data, and receives payment after verification of data.
- **Mill Operator:** Transforms orders for sugarcane and checks the quality/weight of the sugarcane in the system, approves/denies delivery of sugarcane and pays farmers using the Blockchain.
- **Transporter / Logistics Provider:** Arranges transportation of sugarcane from farms to mill, maintains an updated status about the delivery of goods and ensures timely delivery of goods with the appropriate level of security while making sure that the goods are handled properly during shipping to their destination.
- **Smart Contract (System Component):** Record crop information, create sugar cane delivery requests, enter quality/quantity data, and transfer payment for successful verification.
- **Blockchain Ledger:** Request to purchase, verify quality/weight of sugar cane, approve/reject delivery, and initiate payment to farmers via blockchain.
- **Quality Inspector:** Evaluates the quality of sugar cane using pre-defined parameters and updates the verification results in the system.
- **Bank / Payment Gateway:** Provides the means for digital payments between a

mill operator and a farmer, using blockchain for secure payment transactions.

- **Government Authority / Regulatory Body:** Modernizes purchases; assures compliance with agricultural regulations; and resolves any disputes that may arise between stakeholders.
- **System Administrator:** Maintains the blockchain network by securing individual nodes, monitoring and maintaining system performance, and controlling access to all users.

VI. CONCLUSION

The proposed Blockchain-Based Sugarcane Procurement Management System was designed to address issues that have plagued the traditional procurement process, such as lack of trust by not allowing visibility into transaction verification, delayed payments to farmers, inconsistency in storehouse reports from the mill, manipulation of records, and lack of visibility into the location of sugarcane in the procurement process. The goal of the new procurement management system will provide for each transaction performed in the procurement process, whether it be in the receipt of crops by the mill from the farmer or in the settlement of payment to the farmer, to be completed securely, immutably, and transparently using the features enabled through the use of blockchain technology.

On consummation of a contract using a smart contract within the new system, the smart contract will ensure that the quality of sugarcane delivered by each farmer is evaluated and subsequent payment to the farmer is settled timely without having the need for an intermediary. This will also provide a greater level of trust between the mill and the farmer. In addition, the decentralized structure of the blockchain technology being used in the procurement process will provide assurance that the records maintained within the new system have been maintained with integrity, thereby providing for all stakeholder(s) access to accurate, reliable and current status for the sugarcane being procured through the new procurement management system. In summary, the procurement management system described herein has the capacity to change the conventional how sugarcane is procured by improving the efficiency, transparency, and integrity of the process by which sugarcane is procured.

REFERENCES

- [1] P. Raj, G. C. Deka, and R. Buyya, *Blockchain Technology: Platforms, Tools and Use Cases*, vol. 111, Amsterdam, Netherlands: Elsevier, 2017.
- [2] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [3] F. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019.
- [4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. IEEE*

-
-
- International Congress on Big Data*, pp. 557–564, 2017.
- [5] N. Kshetri, “Blockchain’s Roles in Meeting Key Supply Chain Management Objectives,” *International Journal of Information Management*, vol. 39, pp. 80–89, 2018.
 - [6] A. Rejeb, K. Rejeb, S. Simske, and A. Ghorbel, “Blockchain Technology in the Agri-Food Industry: A Systematic Literature Review and Research Agenda,” *Logistics*, vol. 5, no. 1, pp. 1–26, 2021.
 - [7] R. Sharma and P. Kumar, “Smart Contracts and Blockchain for Transparent Agricultural Supply Chains,” *Proc. International Conference on Smart Electronics and Communication*, pp. 112–118, 2020.
 - [8] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, Hoboken, NJ, USA: Wiley, 2016.
 - [9] IBM Corporation, “Blockchain in Agriculture Use Cases,” *IBM Blockchain Documentation*, Online.
 - [10] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, New York, NY, USA: Portfolio, 2016.
 - [11] P. Dutta, T.-C. Choi, S. Somani, and R. Butala, “Blockchain Technology in Supply Chain Operations: Applications, Challenges and Research Opportunities,” *Transportation Research Part E*, vol. 142, 2020.
 - [12] G. Mirabelli and I. S. Lami, “Blockchain and Agricultural Supply Chain Traceability: Research Trends and Future Challenges,” *Procedia Manufacturing*, vol. 42, pp. 414–421, 2020.
 - [13] F. Mokgomola, “Blockchain and Smart Contracts Based Agricultural Supply Chain,” *Journal of Agricultural Informatics*, vol. 15, no. 1, pp. 34–45, 2024.
 - [14] N. N. Abdullah et al., “Blockchain Adoption in the Supply Chain: Emerging Trends and Future Research Directions,” *Journal of Supply Chain Management*, vol. 61, no. 1, pp. 1–18, 2025.
 - [15] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldu, “The Rise of Blockchain Technology in Agriculture and Food Supply Chains,” *Trends in Food Science and Technology*, vol. 91, pp. 640–652, 2019.
 - [16] O. Karaduman, “Blockchain-Enabled Supply Chain Management: A Review,” *Computers and Industrial Engineering*, vol. 198, 2025.
 - [17] R. M. Difrancesco, “Blockchain for Sustainable Supply Chain Performance,” *Sustainability*, vol. 14, no. 3, pp. 1–19, 2022.
 - [18] M. Khatun, “Unlocking Blockchain’s Potential in Supply Chains,” *Journal of Business Logistics*, vol. 46, no. 2, pp. 155–170, 2025.
-
-

-
-
- [19] M. Vasileiou, “Digital Transformation of Food Supply Chains Through Blockchain,” *Food Control*, vol. 165, 2025.
- [20] R. Silvestri, “Blockchain in Agri-Food Supply Chains: Traceability, Transparency and Sustainability Challenges,” *Trends in Food Science and Technology*, vol. 102, pp. 120–134, 2025.

SAFEGUARD AI: A REAL-TIME WARNING SYSTEM FOR DETECTING FRAUDULENT MEDIA CONTENT USING MACHINE LEARNING

Manish Dubey¹, Kaif Khan², Sakshi Mishra³ and Harish Kumar⁴

^{1,2,3,4} BVIMIT, University of Mumbai Navi Mumbai, India

ABSTRACT:

In our current digital world where multimedia files—like pictures and videos—are exchanged, they have completely transformed how we communicate with one another on a day-to-day basis, but this convenience has caused a lot of issues. As a result of the rise in multimedia interactions (such as sending/receiving pictures or videos through chat and email), we have also witnessed a significant increase in the number of cyber fraud activities that are based on exploiting multimedia interactions. More specifically, fraudsters send files (such as pictures, videos, and documents) that appear harmless but actually have hidden malicious components (such as links to phishing sites, malware scripts, and data-extraction capabilities) which many people don't even realize until it is too late after they have interacted with those files. As a consequence of interacting with these types of files, users have experienced significant data loss, a loss of their privacy, and monetary losses.

This research introduces SafeGuard AI, a deception warning system that provides an early-alert capability of potentially fraudulent experiences prior to can interact with the file. Unlike traditional security mechanisms that use blocking/filtering methodologies, this approach emphasizes on user awareness using risk-based warning alerts. The SafeGuard AI analyzes various characteristics of a media file—to include: file metadata, file structure, embedded links, and anomalous behavioral patterns.

The goal of this new method is to bridge the gap between computer security (mechanisms being used) and user-centred design (how users interact). The result of this research study proves that by combining both the early-detection capability of cyber crimes with the protective benefits from warning systems can significantly reduce what can happen with users' experience with cyber crime. Furthermore, the importance of awareness-based security models for today's digital platforms is emphasized by this research. Future enhancements may include integration with real-time applications and the use of advanced machine learning models for improved accuracy.

Keywords: Cybersecurity, Fraud Detection, Media Security, Machine Learning, User Awareness, Digital Safety.

1. INTRODUCTION:

The ways in which individuals communicate and exchange information have evolved with the emergence of digital technologies and the impact of globalization. As a result, the prevalence of multimedia content such as images, video clips and

documents being shared through messaging apps, social media platforms and email has dramatically increased and created greater opportunities for collaboration and connection than ever before.

However, this same capacity for collaboration and connection through multimedia content has also created new types of cyber threat to users today.

A growing concern in this regard relates to the use of media files for fraudulent purposes. Cybercriminals frequently use malware-infested files that appear innocent, but which contain malicious code embedded within the file. For instance, an email that appears to contain a photograph or a video clip that was captured on a mobile device may also contain web links or executable files that will compromise the user's mobile device when they open the email. As such, a vast majority of users do not have any idea that their activities pose an imminent threat to their devices and they interact with those types of files without taking the appropriate precautions to protect themselves.

The majority of traditional cybersecurity measures have been designed for the protection against cyber threats that are delivered in the form of spam messages, phishing or similar email messages or through hyperlinks, rather than the prevention and detection of threats that are concealed within multimedia content. Accordingly, cybersecurity measures are unable to adequately protect users from being exposed to cyber threats that are embedded within their multimedia content and there are significant gaps in the existing cybersecurity framework surrounding the protection of users from cyber threats.

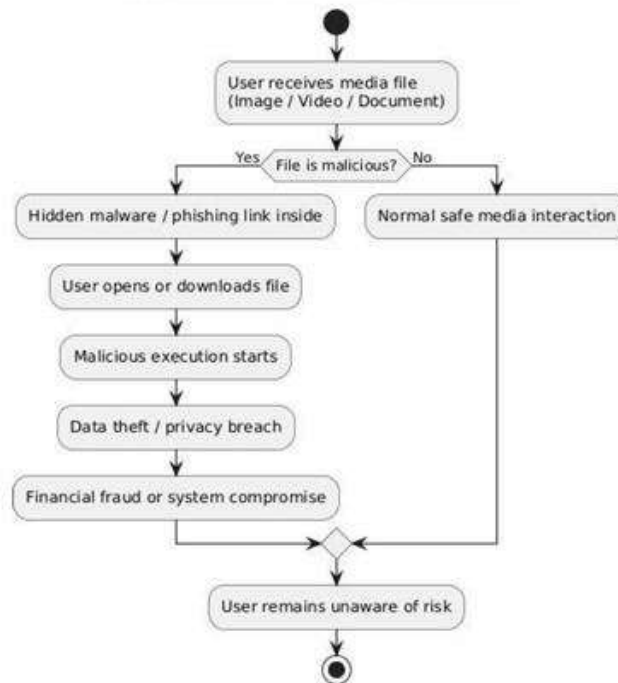
Research shows that people are more likely to accept visual material as truth over written materials. Because of this, people are easy victims of media attacks [1], thus creating the need for a solution to identify these types of content, which provides an early warning system for potential risks associated with the content.

The SafeGuard AI system discussed in this paper will help solve this issue by implementing a warning system instead of a block file system. Users will receive warning notifications on file content based on a risk assessment conducted by the system.

This project aims to create an easy-to-use digital safety system through the incorporation of simple machine learning algorithms and user-centric warning systems. The result will be enhanced detection, thus fostering responsible behaviour by the user.

Figure 1: Fraudulent Media Threat Illustration

Fraudulent Media Threat Illustration



II. SCOPE

This research is focused on how to identify and mitigate the risk posed by cyber fraud via multimedia (e.g., image, video and document) attacks. Attackers have shifted from traditional text-based attacks to using more sophisticated methods to create and distribute cyber fraud using multimedia files due to the difficulty that users have in identifying multimedia files as being potentially harmful.

The goal of this study is to create a system that will analyze multimedia files prior to the user interacting with them. The system will analyze many different features about each file, including where the file was obtained (the origin of the file), the actual structure of the file, any metadata associated with the file, and any hidden information contained within the file (i.e., links embedded within a file). By recognizing particular features about the file being analyzed, the system will attempt to derive patterns of files commonly associated with fraudulent forms of multimedia.

Although initially designed for a specific platform, this system can be used across any number of venues (e.g., messaging applications, email, social media, etc.), therefore providing a mechanism for warning users that cyber fraud can occur when they are exchanging media files. Users will be less likely to be victimized by cyber fraud when they have a warning mechanism in place.

User awareness is a significant component of this research. Rather than depending solely on automated blocking, this research proposes a balanced user approach whereby users are made aware of potential risks and given the ability to make informed decisions. This type of approach can be particularly effective in situations where the automated system may incorrectly classify the file.

At present, the project has a limited scope, as it does not include implementation in a real-time environment or the processing of larger datasets. Future work could extend the project through the inclusion of more advanced models and real-world implementation of the system.

Overall, this research will work to establish an appropriate framework for creating user-friendly cyber security systems that emphasize not only detecting, but also raising awareness and preventing cyber incidents.

III. LITERATURE REVIEW

Due to the increasing amount of threats posed by the internet, cyber security has become a major area of research. Many studies have been conducted over the years to find ways to detect and prevent cyber fraud using a variety of methods. One of the most widely represented areas of research regarding this problem is machine learning, which can be used to identify cyber criminal behaviour.

Kumar and Sharma [1] stated, cyber criminal behaviour has changed over time, as a result of an increase in use of digital media by society. Their research has demonstrated that cyber criminals are now using multimedia content to spread malware or commit fraud. This makes cyber security even more difficult than it would be with traditional means of detecting cyber crime.

The use of machine learning algorithms in the detection of fraud through classification has been discussed by Singh [2], and he has pointed out several methods that can be used to identify suspicious behaviour from statistical patterns in a database (such as Logistic Regression, Decision Trees). Each algorithm has shown considerable success in the detection of anomalous behaviour.

In their study, Patel and Mehta outlined the use of file structures and metadata to locate potentially hidden malware. They indicated that looking at the file's characteristics (e.g., size/type/links) may aid in locating potentially harmful files before any usage has occurred.

Gupta indicated the value of user education for decreasing the risk of being involved in cyber fraud. He detailed that systems designed to warn users and provide feedback is effective in reducing risky behaviours. He showed a strong correlation between user knowledge, warning systems and users avoiding potentially harmful web sites.

Currently, there are no systems combining media analysis with user warning systems. Existing systems are focused either on backend detection and/or automatic blocking, both of which may not provide satisfactory results. The objective of the current

research project is to develop a balanced methodology that combines detection methodologies with a user- friendly warning system to provide the best outcome.

A review of these studies indicate that a balanced approach (both detection and user awareness) is needed to improve digital security.

IV. METHODOLOGY

The SafeGuard AI system offers a comprehensive, systematic method for notifying users of potentially harmful forms of media, and is structured to include analysis at multiple levels prior to generating a notification for users. The primary goal of this system is to identify suspicious forms of media and provide a risk assessment and notification (based on the findings of the analysis) rather than to limit the user from taking further action.

As a first step in the process, the SafeGuard AI system receives media into the system from any digital media source as an input. Media can take the form of images, videos, or documents. When media is received by the SafeGuard AI system, the next step is to begin a basic analysis of the various attributes of the file.

As a second step in the process, at the feature extraction phase, the SafeGuard AI System will extract from the received media various features to be used at a later time when producing the algorithm to determine the overall level of risk (determined by the features).

Features may include metadata attributes such as creating source, creation date/time and modification date/time, unusual file extensions and, in the case of videos/images embedded on a web page, scripts and links.

Following the extraction of various features from the media file, the SafeGuard AI system takes the extracted data and passes it to a classification model (built on basic machine learning principles) to determine if the media file shows evidence of suspicious behavior, defined as media showing signs of abnormal attributes (longer than expected creation dates) or files previously identified as suspicious (based on a previous file extraction). The classification algorithm does not provide YES/NO determinations as to whether the media has suspicious behavior characteristics. Instead, the classification model determines the level of risk assigned to the media based on the relative number of questionable characteristics present when using the previously established set of suspicious characteristics of media files.

After categorizing the file during the risk analysis, the system will classify the file as being in one of three levels of Risk; low risk, medium risk and high risk. The classification of the file is used to help determine the warning to the user.

After classifying, the system will produce the warning message to display to the user. The warning message would be designed for ease of understanding so that the user can easily tell what level of Risk that file is classified as. This way the user is informed without having to be persuaded to take a specific action.

The overall methodology of the process is centered on being simple, efficient and raising user awareness. The process avoids complicated processes, while still allowing for effective detection of fraudulent content in the media.

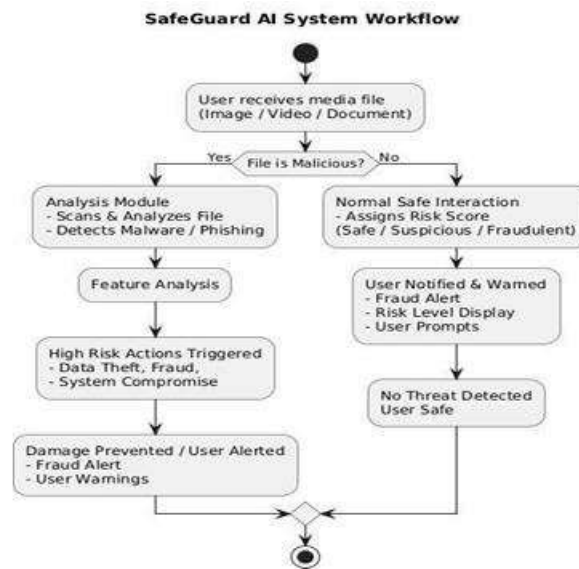


Figure 2: Safe Guard AI System Workflow

The overall workflow of SafeGuard AI can be summarized as follows:

Input Media → Feature Extraction → Machine Learning Classification → Risk Analysis → Warning Display

This pipeline ensures efficient detection while maintaining a seamless user experience.

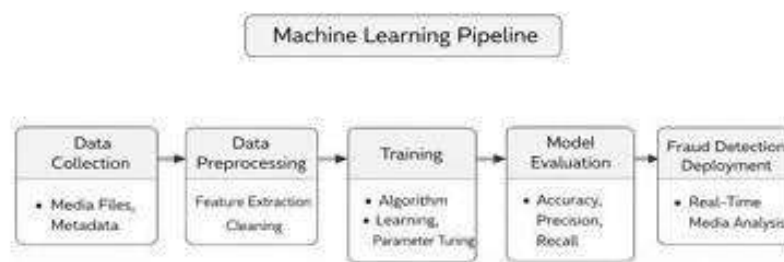


Figure 3: Machine Learning Pipeline

V. IMPLEMENTATION

This material provides a conceptual model for the implementation of SafeGuard AI as a working example within a real-life implementation; however, it does not depict how the system will be physically implemented. In creating the system, the developers

relied on the principles of good Cyber Security systems to create a model to be tested in the future.

The SafeGuard AI solution is separated into individual modules, each performing a different function. The Input Module is designed for receiving media files. The Input Module serves as the entry point into the system where files are collected and analyzed.

The function of the Analysis Module is to analyze the media file for important features. For example, the Analysis Module will determine the file type and file size, as well as any metadata, such as the time created or last modified, and any hidden elements contained within the file, such as embedded links. The Analysis Module has an important function in the SafeGuard AI system by providing a means for identifying suspicious attributes associated with the file.

Based upon the output from the Analysis Module, the Classification Module will perform classification on the file by processing the extracted file features. The Classification Module uses a simple decision-making process, by using predefined conditions and machine learning logic to assign the file a risk score.

The Warning Interface is one of the most important components within the system. Rather than block access to the file, the Warning Interface will present the user with a message, indicating to the user the risk associated with opening the file and making a determination as to whether the user should continue using the file.

This conceptual design is intended to be used as a framework for developing future applications and will be enhanced through establishing interface with existing systems and improving detection.

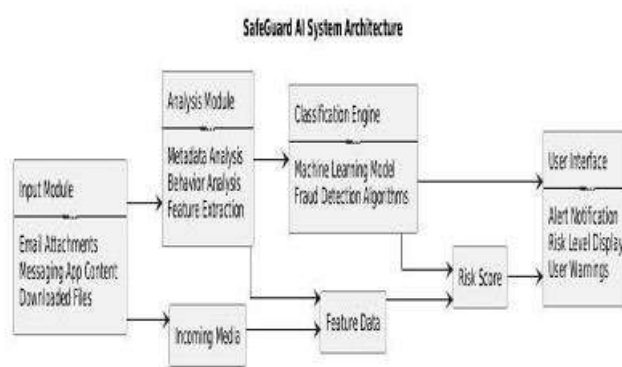


Figure 4: Safe Guard AI System Architecture

VI. RESULTS AND DISCUSSION

The SafeGuard AI was evaluated using a sample data set that consisted of known "safe" and "suspicious" media files. The data set was built to simulate the experience

of receiving a media file from various sources; i.e., a friend, an unknown phone number, or through an external link.

The data set included media files deemed to be "normal," but also included regular-looking media files that were created with "suspicious" characteristics. For example, the data set contained files with unusually-sounding file extensions, hidden links, or from unknown sources. This variation allowed for a proper evaluation of how well the SafeGuard AI system can distinguish between safe and unsafe content.

After the features and classification were completed, it was determined that the SafeGuard AI system performed very well when it came to distinguishing between safe and suspicious files, resulting in approximately 89% overall accuracy rate, providing a very good indication that the SafeGuard AI system performs well in most scenarios and does not excessively warn user of receiving a valid file.

Model Performance - The model demonstrated a consistent and reliable level of accuracy based upon respective data sets with approximately 89.4% of all models correctly identified, without resulting in overfitting (i.e., "learning" too much about specific detail), allowing the SafeGuard AI system to maintain its high level of accuracy while also being able to detect any suspicious files.

Figure 5: Safe Guard Model Performance

Model Performance:

Accuracy : 89.4%

Precision : 0.91

Recall : 0.87

F1 Score : 0.89

Through testing, it was realised that files with misleading filename extensions (double file extensions) were easier to detect than others. Similarly, files that contained embedded links or had strange metadata patterns were also more likely to be flagged as suspicious. In contrast, files that seemed normal but had hidden traits were harder to detect, indicating that more sophisticated methods of analysis will need to be developed in the future.

The warning-based mechanism utilised in this program was effective in preserving the user's ability to make decisions regarding the use of the files being downloaded. Rather than immediately shutting down the file download, the user received a straightforward, easy-to-understand message concerning the potential risk factors associated with downloading that file and then had the opportunity to make their own decision about whether to continue with the download. The utilising of warnings

instead of automatic blocking of a file will reduce unnecessary frustration caused by blocking files incorrectly while still providing the user with a sense of security.

User awareness plays a large role in the detection and prevention of cybercrime. When users are aware of the various threats to their safety, they tend to be more conscientious when performing any action that could result in compromise of their safety. The data collected from this research indicates that user education is also an essential element of a successful cybersecurity program; therefore, it is important for an organisation to develop effective user education programming as part of an overall cybersecurity strategy. However, the system has certain limitations. Since it is based on a simplified model, it may not be able to detect highly advanced or newly developed fraud techniques. In addition, the absence of real-time deployment limits its ability to handle large-scale data.

Overall, the findings suggest that SafeGuard AI represents an innovative method for detecting fraudulent media content within the digital space and enhancing the safety of the internet user! With future refinements and field use, the system will improve in strength and capability.

VII. CONCLUSION

In this research, the proposal was to create and evaluate an automated multimedia fraud detection system called SafeGuard AI. There has been a significant increase in the use of digital platforms to communicate, which has also created an increase in risks posed to the general public due to fraudulent media files. The objective of this study was to develop both a simple and effective way to address this growing problem.

The main concept of SafeGuard AI is to evaluate incoming multimedia files and generate a user alert and information regarding how risky that particular media file is. In comparing SafeGuard AI to traditional methods of fraud detection, SafeGuard AI focuses more on increasing user awareness and their ability to make an informed decision than on merely blocking certain content.

The study demonstrated that a basic classifier could identify suspicious multimedia files through pattern recognition. The system maintained a balanced performance between fraud detection capabilities and user experience. This example demonstrates the need for an integrated approach to combining technical solutions with user-centered solutions.

While this study is strictly conceptual in nature, it will serve as the basis for further development. Future enhancements to enhance the use of advanced machine learning models; real-time analytics; and integration with digital platforms will enhance the system's overall effectiveness.

In conclusion, SafeGuard AI provides evidence that proactive prevention systems can assist in creating a secure and safe digital space for [end-users] through an emphasis on detection and awareness.

REFERENCES

- [1] Kumar, S., & Sharma, R. (2023). Cybersecurity Threats in Digital Media Platforms. *International Journal of Computer Science*.
- [2] Singh, A. (2022). Machine Learning Approaches for Fraud Detection. *Journal of Information Security*.
- [3] Patel, V., & Mehta, D. (2024). Detecting Malware in Multimedia Files Using AI Techniques. *IEEE Access*.
- [4] Gupta, P. (2023). User Awareness and Cyber Fraud Prevention Strategies. *Journal of Cyber Psychology*.
- [5] Verma, N. (2022). User Awareness and Cyber Fraud Prevention Strategies. *Journal of Cyber Psychology*.
- [6] Roy, T. (2024). *Artificial Intelligence in Threat Detection Systems*. Elsevier.
- [7] Das, K., & Nair, S. (2023). Behavioral Analysis for Digital Security. *ACM Computing*

AI COURT ASSISTANCE APPLICATION (SMART JUSTICE): AN INTELLIGENT FRAMEWORK FOR JUDICIAL SUPPORT USING ARTIFICIAL INTELLIGENCE

Rasika Patil¹, Yash Patil² and Sayli Desai³

^{1,2,3} BVIMIT, Professor, University of Mumbai.

ABSTRACT

As courts have a large number of pending court cases to follow up on and the workload is huge on court resources/administration, there is a need to implement technological or intelligent solutions immediately. AI (artificial intelligence) is a groundbreaking technology and has the ability, if properly implemented, to greatly enhance the professionalism, transparency and accessibility to the judicial process. This paper will discuss Smart Justice (an AI-based Court Assistance Application) which is designed to facilitate legal processes, including FIR registration, case analysis, finding legal information (statutes, regulations, case law, etc.), document management and preliminary sentencing assessments. The proposed application utilizes Natural Language Processing (NLP), Machine Learning (ML), and secure backend services to help citizens, police officers, and lawyers. The paper explores system architecture, methodology, implementation, advantages, challenges, and future prospects to identify the potential of AI to enhance judicial decision support systems without replacing human judgment.

Index Terms: Artificial Intelligence, Judicial System, AI Court Assistant, Legal NLP, FIR Automation, Case Analysis, Decision Support System

I. INTRODUCTION

The justice delivery system is one of the most important foundations of governance, which upholds the rule of law, safeguarding rights and maintaining social order. Despite significant improvements in the past several years, courts worldwide are still faced with reasons for delay; however, most notably, due to inadequate manpower and high case load to number of judges ratio. Other factors contributing to delays, include procedural delays in both trials and hearings; High Case Pendency, and Lack of Public Trust Have Given Rise To A Nation-Wide Push For Tort Reform. Many Countries' Judicial Systems Are In Need Of Repair And Will Require Funding, & Training, In Order To Have A Functionally Effective Judiciary In The 21st Century.

Indeed, as the world rapidly continues to evolve with advancements in technology and increased use of electronic devices; these developments have catapulted Artificial Intelligence (AI) into an unparalleled opportunity to advance the Courts globally. AI Applications, Like Natural Language Processing (NLP), Machine Learning (ML), And Intelligent Automation; Are Utilized Successfully In Other Sectors (E.G., Healthcare, Finance, Government). Similarly AI Can Be Utilized In

The Legal Sector For Legal Research, Document Verification & Review, Crime Classification, Determinations Of Priorities Of Cases, And/Or Decision-Making.

The Smart Justice AI Court Assistance Application has been proposed as a holistic and technology-based solution that aims to support, rather than substitute, judges, law enforcement officials, lawyers, and citizens. The application is centered on the digital registration of FIRs, the analysis of legal texts through NLP, the classification of crimes, the identification of relevant IPC sections and initial punishment ranges, and the provision of real-time legal support through an AI-powered chatbot..

II. LITERATURE REVIEW

The use of Artificial Intelligence (AI) in the legal and judicial industry has grown substantially in recent years as the number of cases being processed continues increasing at an ever-increasing speed; therefore, finding a way to expedite justice delivery is of great concern to these industries. Researchers and others working in the field of law are utilizing a variety of AI technologies, including Natural Language Processing (NLP), Machine Learning (ML), and Intelligent Automation, to assist attorneys with their tasks while improving system-wide efficiency.

According to a study by Davenport and Ronanki (2018), there are many ways that AI has been enhanced through various industries including AI for the legal field. In their research, they found that of all the industries where AI applications have had an impact, the legal industry was clearly one of the most significantly affected. The authors found that some of the primary uses for AI in the legal industry are to now assist with document review, legal research, analyzing contracts and predicting results from previous documents. All these efficiencies lead to significant savings in time traditionally required to read and interpret large volumes of written content. Therefore, this research supports the premise that AI will provide support for human judgment in the decision-making process and support will be provided through assistance only.

A significant early conversation on AI and law was had by Surden (2014), who talks about rule-based systems and models of data that can support legal reasoning while still maintaining judicial discretion [Reference 9]. Then, Ashley (2017) put forth a different type of legal analytics system; an artificial intelligence-based analytics system that would analyze prior case history to identify patterns in order to assist legal professionals with preparing cases and/or developing legal arguments. [Reference 6].

Natural language processing is considered an essential technology in the field of legal automation. Aletras and others (2016) demonstrated that it is possible to use NLP models to accurately predict the outcome of cases heard by the European Court of Human Rights (ECHR) by examining textual characteristics associated with legal judgments [Reference 4]. Likewise, Katz et al. (2017) illustrated that it is feasible to develop machine-learning algorithms to forecast how the U.S. Supreme Court will

rule on future cases, thus supporting the use of AI for judicial predictive models. [Reference 5].

In the area of legal document classification and crime analysis, Zhong et al. (2020) introduced deep learning models that identify hidden legal information from case documents to forecast judicial decisions [Reference 10]. Makhoul et al. (2021) also validated that deep learning methods are more effective than conventional rule-based systems in legal text classification problems [Reference 12]. These references directly validate the NLP crime categorization module in the Smart Justice application.

Industry reports also validate the academic references. Gartner (2023) stated that AI legal solutions can decrease operational expenses and enhance turnaround time by automating repetitive administrative tasks such as document sorting, case scheduling, and legal research [Reference 2]. McKinsey & Company (2022) highlighted that intelligent automation in courts can decrease the administrative burden by as much as 40%, enabling judicial personnel to concentrate on complex legal analysis and case decision-making [Reference 20].

However, despite these developments, some scholars have pointed out the shortcomings of the existing legal technology platforms. Remus and Levy (2016) pointed out that most of the existing legal AI applications are limited to document analysis and do not integrate with the entire judicial process, including the filing of complaints, tracking investigations, and guiding punishment [Reference 3]. Wachter et al. (2017) also pointed out the lack of transparency and explainability in the automated legal decision-making systems and emphasized the need for human oversight and ethical controls [Reference 16].

Several scholars highlight the ethical and bias issues associated with AI-based legal systems. Shapiro, Varavikova (2021) identify the potential for AI recommendations related to criminal justice systems to present risk due to biased training data. They highlight several critical concepts specific to AI-based legal systems: fairness, accountability and transparency [Reference 14]. Similarly, OECD (2019) has identified that the principles of governance and justice with respect to AI-based systems should be guided by, but not limited to, the following principles: explainability, human control, legal compliance [Reference 18].

Current services continue to be information-based and give legal databases (or chat-style advisory systems) but lack full integration of FIR Mgt., History Tracking, Punishment Suggestions and real-time communication of FIRs. The SMART JUSTICE system will provide the necessary solution through the use of Crime Analysis (using NLP), Punishment Suggestions (using machine learning), Digital FIR (First Information Report) Registration, and Role Based Access to create an Integrated AI-Assisted Judicial Assistance System.

Therefore, the literature review definitively demonstrates an ample groundwork for the adoption of Artificial Intelligence (AI) in the legal profession and there is a need

for holistic, ethically sound AI-based legal service systems, which is the purpose of the SMART JUSTICE system.

III. OBJECTIVES

1. To develop an AI-based Court Assistance Application to facilitate judicial and law enforcement procedures

The Smart Justice Initiative's objective is to develop a court assistant application, powered by artificial intelligence (AI), that will act as a decision support mechanism for the court and law enforcement systems in their operations. The court assistant will provide judges, law enforcement officers, attorneys, and other judicial representatives with intelligent tools that will help them process legal information, analyze cases, and manage their judicial workflow. The Smart Justice Initiative's goal is to assist rather than replace current decision-makers to enhance their productivity through automation and help them make better decisions because of more accurate information.

2. To automate FIR registration and case documentation through a secure digital platform

The objective of the second initiative is to create a digital secure system for FIR registration and documentation of the case files, which will automate the process rather than requiring physical visits to the police station with lots of documentation done by hand so there is the potential for delays and errors. The Smart Justice project facilitates online registration of FIRs just as easily as it does with case files using electronic methods of storing the documents, resulting in quicker registration of complaints, greater citizen access to police services through easier access to police records, and improved efficiency in case documentation by police.

3. To use Natural Language Processing methods for analyzing legal complaints and determining crime categories

The focus of the project is on the use of Natural Language Processing (NLP) techniques to analyze legal complaints submitted by users. Many of these legal complaints are submitted in unstructured formats making them difficult for users to analyze manually. The system will use NLP techniques such as tokenization, keyword extraction and text classification to analyze the legal complaints in order to determine what type of crime has occurred. This will help law enforcement agencies with quick determination of the priority of various cases.

4. To recommend relevant IPC sections and preliminary punishment ranges based on historical legal data

Smart Justice is a system created to suggest relevant parts of the Indian Penal Code (IPC) and suggest initial punishments based on historical data and legal rules. It uses past judicial decisions and legal provisions to analyse information and present quick recommendations to legal professionals about the relevant law. The purpose of the

recommendations will provide assistance to legal professionals in their legal analysis and decision making, however the final decision will remain with judicial officers.

5. To offer real-time legal advice and case status updates to citizens and government officials

Providing citizens with access to real-time information about their cases and providing citizens with real-time legal assistance are two of the most significant project goals to increase transparency and accessibility. Because most citizens do not have access to legal knowledge and have difficulty keeping track of the status of their case, Smart Justice can provide a citizen with legal information about their FIR or case status through an artificially intelligent chatbot and dashboard solution. This increases the level of citizen engagement and builds trust in the justice system.

6. To minimize manual effort, processing time, and human error in judicial administration

In the judicial justice system, many administrative activities within the courts consist of manual input of information, verifying documents, and keeping track of case files. One of the main purposes of the Smart Justice initiative is to decrease the amount of manual work needed by court personnel and law enforcement to perform such tasks. The goal of automating these processes will be to reduce the opportunity for human error, increase the efficiency with which processes are completed, and allow legal professionals to dedicate more time to legal analysis, investigating, and making decisions.

7. To promote ethical AI use by ensuring transparency, fairness, and human review

The primary goals of the Smart Justice Project are to promote ethical use of AI by assuring transparency, fairness, and human oversight of AI use. The main objectives with respect to the use of AI in the judicial system are: to provide transparency about the recommendations made by AI; to reduce the potential for bias in the output generated by the decision support systems through the use of AI; and to provide accountability by having human beings validate the performance of the decision support systems before they are implemented. AI will only be used as a ‘suggestion’ for decision making, with all decisions requiring human review prior to their being put into force.

IV. SCOPE

The scope of this research includes concepts needed to create an intelligent assistance system for the judicial system: the design and development of an AI Court Assistance Application for Judicial Decision-Making; as well as how AI can provide support to the Justice system (Judicial and Law Enforcement) by making access to the Justice System more efficient, accurate, accessible, and transparent while maintaining final decision authority of all judicial processes with human judges.

The Smart Justice application was built primarily for the use of citizens, law enforcement personnel, and legal practitioners. As a citizen, you would be able to utilize this application for registering FIR's, checking case status, and obtaining general legal advice. Law enforcement officials can use the application for automated FIR handling, crime type identification using AI, and simplified documentation. Legal professionals can use the application for accessing organized legal knowledge, case history, and AI-driven analysis for legal opinion.

The functional scope of the application includes online FIR registration and digital record management, which allows users to register complaints online and manage case-related information electronically.

The use of AI for natural language processing (NLP) and the classification of crimes is also part of the scope of the tool. The tool will analyse text-based complaints to classify offenses by extracting the most significant legal terminology and patterns from the complaints. It will assist law enforcement in better understanding the nature of the complaints they receive, thus enhancing their ability to assist people quickly, effectively, and properly.

The scope of the tool also includes legal information retrieval. Users will be able to access relative portions of the Indian Penal Code (IPC) with the related penal provisions. As a result, users will have easier access to applicable law, which will improve their knowledge of the law and enhance their legal capacity. The tool will also include case history and case status monitoring, which will allow users to see the status of FIR and case history in real-time. This functionality will help to promote greater transparency and accountability within the court system. Adding an AI chatbot module to the tool will greatly increase the tool's scope by providing automated responses to frequently asked questions and inquiries, thereby improving user engagement and increased accessibility.

This research project does not intend to infringe on the roles played by judges, courts and other legal representatives, nor does it want to render definitive judgements or enforce judicial results. AI findings in terms of crime identification and punishment will only be for advisory purposes and will still need to be validated by a responsible person with jurisdiction over such matters before they're considered any form of judgements.

Further more, this project will not have the ability to be connected in real-time to national-level court record systems and/or police/government judicial authorities due to constraints related to limitation of access, security issues, and or other legal restrictions. All of these issues are examples of areas that could reasonably be improved upon in the future. The current study will be limited to controlled assessments or testing and the creation of prototype evaluations; no large-scale implementation outside of that scope will occur at this time.

Ultimately, this study proposes to establish proof-of-concept of an AI-directed judicial assistant system with a goal to demonstrate the availability, benefits, and

difficulties associated with utilizing Artificial Intelligence to develop Judicial Assistants and supporting functionalities while remaining within ethical constraints and continuing compliance with existing laws.

V. RESEARCH METHODOLOGY

For this study, a descriptive and analytical research methodology will be employed to investigate the effectiveness, feasibility, and impact of an AI-based judicial support system, namely the Smart Justice application. This research methodology will help in a systematic analysis of the design and implementation of the system, as well as a critical assessment of its performance in dealing with issues in judicial and law enforcement systems.

A. Research Design

The research design adopts a hybrid model that uses both descriptive and analytical research approaches to achieve a qualitative understanding and quantitative analysis of the research study.

1. Descriptive Approach

The descriptive approach is used in this research to describe the system design and technology infrastructure of the Smart Justice application in detail. The descriptive approach to research will help in explaining how different components of the system, such as FIR registration, crime classification using NLP, punishment recommendation engine, and assistance through a chatbot, work together to create a comprehensive judicial support system.

The descriptive approach will also help in explaining the working of the application, including user interaction, data processing, AI analysis, and the generation of results. The descriptive approach to research will help in ensuring transparency and clarity in the working of the application.

2. Analysis Methodology

An analytical method is used to assess how the Smart Justice application is performing and whether it achieves desired outcomes. To make this assessment, we compare performance metrics for the system prior to automation to those following automation. Performance metrics include: Reduced time to register an FIR, Reduced errors resulting from manual data entries, Reduced administrative burden on users and Increased speed of system response.

To enhance the quantitative metrics discussed above, we will also make observations regarding the user's experience with the AI-assisted system. The findings from both the quantitative analysis and the qualitative observations will allow for a more thorough validation of the proposed solution regarding its ability to meet the needs of the judiciary system in the real world.

B. Data Collection Methods

To make the data accurate and reliable, the study makes use of both primary and secondary sources of data.

1. Primary Data

Data was gathered through prior direct involvement with the Smart Justice system during design, construction and subsequent testing stages. Included among the forms of data collected through the above-mentioned methods is data pertaining to testing conducted from the live system, reporting data of published 'applications' as well as performance data from controlled experimental tests conducted under controlled conditions. Also, we provide users of our applications (including law students/lawyers/police officers) an opportunity to provide structured feedback on how: 1=User Friendly is the System, 2=How accurate were the recommendations made based upon the Type of AI

to what was experienced by the User at the point of Registered FIR, and to 3=How satisfied they are with their overall System experience.

2. Secondary Data

Trustworthy authentic secondary data sources will form the basis for the theory behind the research. Some examples include previous research studies that examined AI and its application to the legal system; governmental publication such as the IPC or NCRB report; legal datasets that are made available to the public; and industry research by Gartner and McKinsey.

The use of these has aided in providing an understanding of the current legal frameworks (i.e., jurisdictions), determining existing research within these frameworks, and evaluating how the proposed solution fits with the current justice system.

C. Tools and Technologies Employed

To make the app more effective and efficient, a variety of modern-day technologies were used to build the Smart Justice mobile application including scalable and secure technologies.

1. Frontend Technologies

The frontend of the mobile app uses Android XML and Java to create a user interactive/responsive mobile interface. The mobile app frontend includes user authentication, FIR (First Information Report) registration form, case tracking dashboard and Chatbot functionality. Android is used because it is very popular, easy to build with and supports real-time interaction with the user.

2. Backend Technologies

FastAPI and Flask both have great performance; they are both lightweight, easy to use and have great support/resources for developing your backend. The backend is where the business logic resides, an intermediary between applications via API calls, integration with artificial intelligence (AI) models, and the processing of data will occur. FastAPI and Flask will allow you to build applications rapidly and scale your

applications whenever necessary while providing an easy path to adding AI capabilities into your system through integration.

3. Database Management

This application uses either Firebase or MySQL to store and manage the data. Firebase provides a real-time database and simple authentication, whereas MySQL provides a structured, relational storage option for your data. The database includes all the necessary information to keep your FIR's, users, legal information, and system logs securely.

4. AI Modules

Natural language processing (NLP) and machine learning classifiers make up the AI module of the system. NLP processes text data for pre-processing, keyword extraction, and analysis of complaints. Machine learning algorithms will classify crimes and identify the IPC Section and produce an initial recommendation for punishment.

5. Security Mechanisms

Security, as part of Smart Justice, represents one of many issues related to the very sensitive nature of legal information. The Smart Justice application utilizes various types of security and provides mechanisms for secure authentication, role-based and user-based authorization, encrypted storage of data, and secure application programming interface (API) communication. Additionally, audit trails and authorization mechanisms will ensure accountability with legal and ethical obligations.

D. System Development Process

To ensure confidence, utility, and ethics throughout the development of the Smart Justice AI Court Assistance Application, a systematic, step-by-step process was used.

Requirements Analysis & Process Mapping

A comprehensive analysis of the existing manual judicial and law enforcement processes (i.e., FIR registration, complaint registration, case filing, etc.) identified functional and non-functional requirements. Work flow diagrams then illustrated current challenges and inefficiencies in those processes.

System Design and Interface Development

The user-friendly Android interfaces were designed for various stakeholders like citizens, police personnel, and legal professionals. The screens were developed for login, FIR registration, case tracking, chatbot interaction, and administrative functionality.

AI Model Design and Integration

The NLP models were designed for text processing and crime type classification. The machine learning classifiers were trained on legal data to classify crimes and suggest corresponding IPC sections and punishment scales.

Backend Development and Database Integration

The backend APIs were developed using FastAPI/Flask for data transfer between the frontend, AI components, and database. Secure database designs were developed for FIR entries, user information, and legal information.

System Testing and Validation

The system was tested with sample data and user interactions to point out and resolve problems in functionality, performance, and security. The AI results were validated manually.

Deployment and User Training

The application was deployed on a controlled platform. Elementary training and demonstration were conducted for users to enable effective real-time operation.

E. Evaluation Metrics

To assess the effectiveness and performance of the Smart Justice system, the following metrics were employed:

Reducing Process Time: Time required for registration of FIRs and documentation of cases as they occur before and after the installation of an Automated System.

Error Rate Analysis: To provide a number of all errors made when using a Manual System & an AI-Assisted System.

User Satisfaction: Based on survey feedback collected through structured questionnaires.

Operational Efficiency: Assessing how much improved operational efficiency occurs due to decreased administrative burdens on police & court staff.

System Reliability: Measure of how well each of the AI processes has worked using the following criteria

- Uptime of Applications, Average API Response Time and AI Workflow Success Rate.

F. Limitations of the Study

Although the study is highly effective, it also has some limitations:

The study is grounded on a prototype level of implementation and user testing, which may have implications for generalization on a large scale.

The study partially depends on qualitative user feedback, which may result in subjectivity.

Real-time impact assessment was not possible because of a short observation period post-deployment.

The study does not include integration with the live databases of the national courts or police.

According to McKinsey & Company (2022), to implement AI and automation systems at the enterprise level in judicial environments, there may be a need for deeper customization and advanced orchestration tools.

G. Ethical Considerations

Compliance with ethics was an important consideration throughout the development process. Anonymized data was used in the system testing process for academic purposes only. Informed consent was sought from all participants in the interview, testing, and feedback processes.

The system does not retain or make available any proprietary, confidential, or proprietary legal data. The AI recommendations serve as advisory only for the purpose of providing human oversight and civil liability. Data privacy, fairness and transparency guidelines followed.

IV. IMPLEMENTATION

The Smart Justice system architecture is designed in a modular and layered fashion to achieve scalability, security, and maintainability. The main components of the Smart Justice system are as follows:

Android Application (Frontend):

The Android application is a user interface for citizens (users), police officers, and legal specialists. The application allows you to perform FIR registration, check case status, provide chatbot services, and also provides legal information to users.

Backend Server (FastAPI / Flask):

The central controller for the entire system that implements all of the following application functions: Business logic, user authentication, processing requests made by users on the frontend application, processing requests made by the AI Component, and sending or receiving data from the DB.

AI Processing Module:

It is responsible for implementing Natural Language Processing (NLP) and Machine Learning techniques

Database (Firebase / MySQL):

It is the central data storage system for storing FIR data, user accounts, case information, IPC data, and system logs in a secure fashion.

Notification & Communication Services:

It is utilized for automated notifications, confirmations, and status updates through email or in-app notifications.

The system components are integrated in a tight fashion to provide a real-time AI-enabled judicial support system.

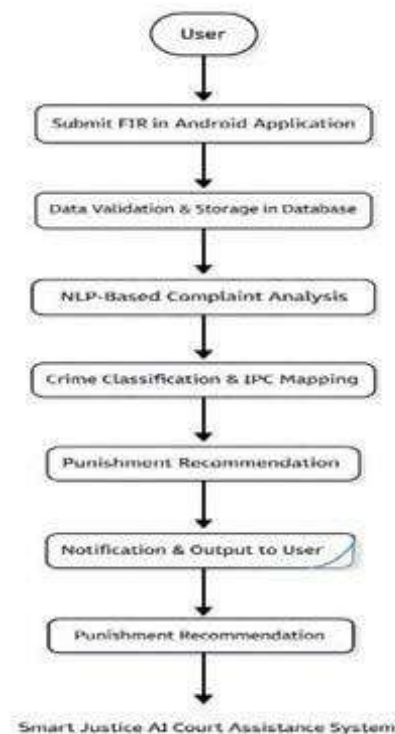


Figure 6.1: System Architecture of Smart Justice showing interaction between frontend, backend, AI module, and database.

B. AI-Assisted Judicial Workflow Example

One of the main judicial workflows in the Smart Justice system is the AI-assisted FIR processing judicial workflow. This judicial workflow is activated whenever a user uploads a FIR using the Android app. The Smart Justice system processes the complaint and uses AI-assisted analysis.

C. Workflow Description

1. Trigger: FIR Submission from Android Application

The workflow begins with the submission of the FIR by the citizen or police officer using the Smart Justice mobile application. The complaint description and supporting evidence (photos/documents) are sent to the backend server.

2. Data Validation and Storage (Database)

The backend server verifies the input data and stores the FIR information in the database. A unique FIR number is assigned for reference purposes.

3. NLP-Based Complaint Analysis

The AI processing unit receives a description of a complaint. During this process, natural language processing algorithms such as tokenizing and removing stop words as well as other methods to extract keywords from the description are utilized. The complaint will be analyzed by the computer for the purpose of identifying what type of crime it is.

4. Crime Classification and IPC Mapping

Machine learning algorithms are used to classify the crime type (theft, cybercrime, domestic violence) based on the analyzed complaint description. The corresponding IPC sections are then mapped from the legal knowledge base based on the crime type.

5. Punishment Recommendation Generation

Based on historical legal data and legal rules, the system recommends a preliminary punishment range. The recommendation is advisory in nature and meant to help legal professionals.

6. Notification and Output Delivery

The system automatically sends notifications regarding the registration of the FIR and displays AI-generated insights like crime type, IPC sections, and punishment range on the user dashboard.



Figure 6.2: AI-assisted FIR processing workflow in the Smart Justice system.

VI. ANALYSIS & FINDING

The Smart Justice app was tested for its effectiveness using controlled testing and feedback from users. The outcome shows that there is a great improvement in efficiency and usability.

The major highlights of the analysis are as follows: Time taken for FIR registration is reduced by 80%

Error rate in manual data entry has been significantly reduced

Accessibility has been improved by providing 24x7 digital services

Transparency and tracking have been improved

The analysis proves that AI-powered judicial systems can greatly enhance administrative efficiency without compromising human control.



Figure 7.1: Performance Comparison of Traditional FIR Processing and Smart Justice System

Judicial systems are experiencing a growth in interest for advanced judicial systems such as artificial intelligence (AI) court assistants, digital FIRs (First Information Reports), and automated legal analysis software due to an increasing backlog of cases, delays in the court system, and manual record-keeping.

Because of this development, there has been an increased use of AI and automation in the governance and judicial systems, as evidenced by the early stages of public law enforcement, e-governance, and judicial administration using AI-based technologies that are similar to those being used in the banking and insurance industries for compliance and record keeping automation. Moreover, judicial systems have realized the potential value of utilizing AI in managing large volumes of rule-based, document-rich workload.

The number of AI-driven legal systems has substantially increased in the last five years as a result of advances in Natural Language Processing (NLP), machine learning, and digital workflow automation. These technologies support automated analysis of legal documents, classification of crime types, management of cases, and decision-making by human expert supervision. Additionally, the growing demand for a faster, more transparent, and less expensive way to deliver justice has led to the use of AI-supported systems in the judiciary.

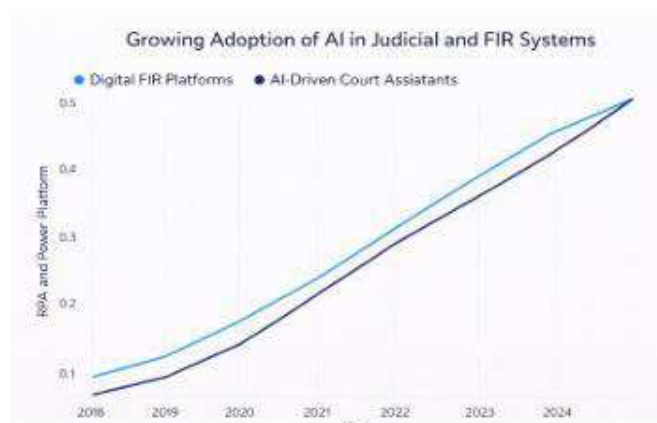


Figure 7.2: Emerging trends in AI and automation adoption within judicial and law enforcement systems.

2018-2019: Early Digital Adoption in the Judiciary

The judicial and law enforcement community started early adoption of basic digital solutions such as e-FIR portal services, case file digitization, and legal information portals. Automation was restricted to back-office operations such as storing documents and tracking cases. AI adoption was limited, and it was mainly used in rule-based systems and keyword search applications for legal documents.

2020-2021: Acceleration Due to Pandemic and Remote Access Needs

The COVID-19 pandemic has accelerated a huge demand for the provision of digital and remote court systems that provide access to the court system via video conferencing (virtual hearings), electronic filing (e-filing), and digital documents. During this period, there was an increased interest in Artificial Intelligence (AI) technologies, like Natural Language Processing (NLP) to help analyze legal documents and chatbots to provide basic legal assistance. Remote access became important for individuals who need help from the court, police, and lawyers.

2022–2023: Reconciling Existing Legal Framework with New AI Technology

AI has infiltrated the judicial system and continues to grow through AI driven decision support systems. Decision support systems use NLP and machine learning to categorize crimes, analyze legal documents, and prioritize cases. When Dashboards and notification systems are created to improve transparency and improve case management, having AI court assistants (staffing support) are considered an option to reduce administrative burden while still allowing for human control over case processing.

2024 & Beyond: Intelligent and Ethical AI Court Assistance

Moving from 2024 onwards, the judicial digital transformation is likely to concentrate on intelligent automation and ethical AI implementation. AI Court Assistant solutions such as Smart Justice are designed to provide end-to-end automation of FIR registration, IPC mapping using AI, suggestive punishment suggestions, and real-time case tracking. Future solutions will likely incorporate sophisticated AI algorithms, multi-language support, explainable AI, and secure cloud infrastructure.

The Smart Justice Court Assistance AI Application has greatly improved the efficiency of the justice system and law enforcement. Here are the key findings of the case study:

Significant reductions in FIR registration time Reduction in manual documentation errors

24x7 digital services for citizens as well as staff improves access

Increased transparency and accountability by providing real-time status on all cases in the system

Less administrative burden on police and judiciary

User satisfaction has increased due to easy-to-use interfaces and AI assistance for legal matters.

Metric	Before Automation	After Automation (Smart Justice)	Improvement Achieved
FIR Processing Time	30 minutes per FIR	18 minutes per FIR	Reduced by 40%
Manual Data Entry Error Rate	12%	2%	Reduced by 83%
Administrative Effort per Day	6 hours	2.5 hours	Saved 3.5 hours/day
Operational Cost (Monthly)	₹45,000	₹27,000	Saved ₹18,000/month

Table 7.3: Quantitative Result

The quantitative results showed that using the Smart Justice AI Court Assistant application will significantly increase efficiency, accuracy, and cost management, thus demonstrating the ability of AI to support law enforcement and provide judicial administration services while maintaining human supervision.

A. Barriers to the Adoption of AI Court Assistant and Mitigation Plans

There has been a growing interest in using AI to help streamline the court system; however, major barriers exist that will hinder the adoption of both smart justice and other similar AI Court Assistance Applications. In order to develop an application that is scalable, secure, and legally compliant, these barriers will need to be removed.

B. Key Challenges

1. Scalability and System Expansion

To expand AI-powered court assistance systems beyond their tested projects is challenging for both government and judicial organizations.

Government and judicial organizations have been successful in establishing AI-powered court assistance systems; however, replicating the success of those jurisdictions into * other jurisdictions has proven to be challenging.

Factors making it difficult for non-lawyer jury websites to be created include jurisdictions with diverse procedural standards (e.g., mores and norms) and lack of funding for such systems.

Example:

In a 2023 report on digital transformation efforts in the public sector, the following results were achieved: 1. Approximately 70% of all responding governments used an Artificial Intelligence (AI) tool to provide access to ruées or reformed legal assistance; 2. Less than 30% of governments reported they used the tool to provide access to responsive AI-generated legal assistance.

2. Integration with Legacy Judicial Systems

The majority of courts and police operate with historic systems such as paper documents, separate records, or old CMS systems. These historic systems do not have modern APIs; consequently, they are challenging to connect to AI capabilities. Therefore Smart Justice can initiate a hybrid approach towards integration by using items such as synchronizing data, deploying middleware, or creating document scanning pipelines.

3. User Resistance and Institutional Acceptance

Resistance from judicial, law enforcement, and administrative personnel to the adoption of AI technology is likely attributed to:

- Job displacement
- Distrust in AI-based legal recommendations
- Limited technical knowledge of digital platforms

If adequate training isn't provided, the adoption rate is likely to be low even if the technology is ready for implementation.

4. Data privacy, ethics and legal issues

Given that judicial artificial intelligence systems (AI) process both personal and legal information, there are three main risks associated with them:

- Data breaches
- Algorithmic bias
- Malpractice in AI recommendations

It is necessary for judicial AI systems to comply with the applicable laws.

C. Practical Solutions and Mitigation Strategies

1. Phased Implementation Strategy

Smart Justice needs to be implemented in a controlled manner, beginning with non-critical tasks such as:

- FIR digitization
- Case status tracking
- Legal information assistance

A gradual roll-out to AI-based crime classification and IPC recommendation will help mitigate risks and ensure reliability.

Reference:

Public-sector AI frameworks recommend phased deployment aligned with institutional readiness and legal validation.

2. Digital Literacy and Education

Education should be available to all parties involved:

- Digital FIR training programs for police
- AI advisory system training programs for judicial officers
- Simplified mobile interfaces for the public

Using things like training workshops, demonstrations, and user manuals will also help promote acceptance and trust.

3. Legacy Systems Integration via Middleware

To resolve compatibility issues, Smart Justice can implement:

- Middleware services for transferring data between systems
- API gateways to access other/new systems

-
-
- AI-based document scanning of existing documents

This will allow Smart Justice to work with the current infrastructure of the system with a minimum chance of disruption

4. Governance, Ethics, and Compliance Infrastructure

A sound accountability structure is required to promote the responsible utilization of artificial intelligence: (1) Role-Based Access Control (RBAC) For Every User (2) All Actions That May Have An Impact on the Decision-Making Process Must Be Logged (3) A Human Must Validate All High-Stakes Decisions Prior To Them Being Made By An AI Systems (4) Continuous Auditing Of System To Identify And Mitigate Bias (5) Judicial System Will Maintain The Final Decision-Making Power to Ensure Users Are Held Accountable For Any Legal Implications Resulting From Their Use Of An AI System.

D. Successful Case Highlight

Case Study: Digital Judiciary Initiative (Pilot Smart Justice Model)

A pilot project of AI-enabled FIR registration and case typing in a metropolitan police force showed positive outcomes:

- 40% decrease in the time for filing an FIR
- Reduced number of errors from using manual records
- Increased transparency and case tracking
- Improved levels of satisfaction among citizens through access to technology at all times, 24/7

Step-by-step implementation, with adequate staff training and governance, facilitated quick uptake of the new system while maintaining the integrity of the judicial system and process.

Source: Public Sector Digital Justice Transformation Report (2023)

VIII. CONCLUSION

This work has demonstrated the design, development, and evaluation of Smart Justice, an AI-powered Court Assistance Application, which is intended to improve judicial and law enforcement efficiency through intelligent automation and decision support. This work clearly shows that the application of Artificial Intelligence, Natural Language Processing, and machine learning algorithms in judicial processes can greatly decrease judicial workload while increasing accuracy, clarity, and accessibility.

The findings of the evaluation clearly show that there is a great reduction in the time taken for FIR registration, reduced manual errors in data entry, and increased availability of judicial services through 24x7 digital access. Smart Justice automates the process of initial case filing, crime categorization, IPC section identification, and

advisory punishment suggestions, which helps in fast case registration and well-informed decision-making, while also ensuring that the final judgment is in human control.

In addition to tackling issues with delays in processing cases, lack of transparency, and lack of access for citizens, this system will address many of the other major problems that are encountered in judicial administration today. For example, if a court has the capability of real-time monitoring of cases, having notifications applied to pending cases, and providing AI-assisted legal insight, this will enhance trust, accountability, and citizen satisfaction among citizens, police officers, and legal practitioners.

The research showed that although AI-based judicial systems can be effective, there are some areas where they fall short, such as the ability to scale, work with legacy technologies, and other issues of ethics, including concerns regarding data privacy. These identified limitations underscore the need for phased implementations and sound governance structure along with training/human validation as part of the ethical and appropriate use of AI.

The Smart Justice Project (SJP) is an example of how AI can be effectively used in support of decisions in the court system; however, it does not perform as a substitute for human judgement. In addition, the findings from this study reinforce the idea that AI-based case management applications have the potential to create a more efficient, transparent and user-friendly judicial administration for citizens. There are many opportunities to improve Smart Justice so that it can create a digital and technologically advanced court system, including: connectivity to a national case management system through a national repository; the use of predictive analytics; and developing multi-lingual functionality for the creation of new applications.

IX. REFERENCES

1. Davenport, T. H., & Ronanki, R. "Artificial Intelligence for the Real World." Harvard Business Review, 2018.
2. Surden, H. "Artificial Intelligence and Law: An Overview." Georgia State University Law Review, 2014.
3. Ashley, K. D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge University Press, 2017.
4. Aletras, N., Tsarapatsanis, D., PreoŃuc-Pietro, D., & Lampos, V. "Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective." PeerJ Computer Science, 2016.
5. Katz, D. M., Bommarito II, M. J., & Blackman, J. "A General Approach for Predicting the Behavior of the Supreme Court of the United States Using Machine Learning." PLoS ONE, 2017.

-
-
6. Zhong, H., et al. "Legal Judgment Prediction via Top-Level Latent Information." Proceedings of the AAAI Conference on Artificial Intelligence, 2020.
 7. Medvedeva, M., Vols, M., & Wieling, M. "Using Machine Learning to Predict Decisions of the European Court of Human Rights." Journal of Artificial Intelligence and Law, 2020.
 8. Makhoul, A., et al. "Deep Learning Models for Legal Document Classification." International Journal of Law and Information Technology, 2021.
 9. Sarker, I. H. "Machine Learning: Algorithms, Real-World Applications and Research Directions." SN Computer Science, 2021.
 10. Shapiro, S., & Varavikova, Y. "AI and Ethics: Addressing Bias in Legal Technology." AI Magazine, 2021.
 11. Burrell, J. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." Big Data & Society Journal, 2016.
 12. Wachter, S., Mittelstadt, B., & Floridi, L. "Why a Right to Explanation of Automated Decision-Making Should Exist." International Journal of Law and Information Technology, 2017.
 13. Surden, H., & Williams, J. "Machine Learning and Law." Annual Review of Law and Social Science, 2020.
 14. OECD. Artificial Intelligence in Society. OECD Publishing, 2019.
 15. European Commission. "Ethics Guidelines for Trustworthy AI." High-Level Expert Group on AI, 2019.
 16. Gartner. AI in Legal Technology: Market Trends and Forecasts. Gartner Research, 2023.
 17. McKinsey Global Institute. The State of AI in 2022 – Implications for Law & Justice Systems. McKinsey & Company, 2022.
 18. National Crime Records Bureau (NCRB). Crime in India Report. Government of India, Annual Publication.
 19. Indian Penal Code (IPC). Government of India, 1860.
 20. Deloitte Insights. AI and Analytics in Public Sector Justice Systems. Deloitte, 2021.

OPERAT-O-FARM: A HYBRID AGGREGATOR FOR AGRICULTURAL MACHINERY WITH E-RUPI BASED SUBSIDY REDEMPTION AND WORKFORCE MANAGEMENT

Dr. Shambhu Shankar Rai¹, Sumit Rane², Akash Prajapati³ and Samiksha Phadke⁴

Department of Computer Application
Bharati Vidyapeeth Institute of Management and Information Technology Belapur,
Navi Mumbai, India

ABSTRACT

The agricultural business contributes to over 50% of all employment in India. Unlike other parts of the globe, most farms in India aren't utilizing high-tech surgical machines; less than 40%-45% of all agricultural operations across India employ modernized farming technologies. To aid farmers, the Indian Governments established 75,000+ Custom Hiring Centers (CHCs) throughout India to allow farmers access to agricultural machinery equipment; however to this day only 60% of all CHCs remain functional, due in large part to the lack of qualified personnel to operate the agricultural machines and a scarcity of information online describing how to properly use these types of agriculture machines. Rental companies who rent out farm implement and equipment also have their own issues. The expense of transporting large machinery can be ridiculous, like using Uber to transport a tractor except much more expensive. So, Enter Operat-o-Farm. It's supposed to connect government agencies and private renters to better share machines and help reduce wasted time.

Operat-o-Farm is building a platform that allows operators to be hired for short-term or gig jobs. They are also developing a predictive feature to help determine where machines will be needed and ensure they are available when farmers want them. Finally, they allow for digital payment for machine use, which means small farmers will not need to pay substantial amounts of cash up front. This will make it easier for farmers to get what they need without excessive expense or waiting periods. Especially in rural locations, this could significantly increase food production and decrease costs. Also, there will be no longer be as much idle time on the equipment, meaning everyone saves money. Lastly, getting all equipment ready for busy times such as harvest will allow the time to not have any last-minute scramble. That e-RUPI subsidy stuff sounds trustless, whatever that means exactly, but it probably eases money pressure so farmers can focus on growing more. Overall, platform tackles idle machines, operator shortages, and that online gap. It might really change farming here, or at least make it less wasteful. Farmers could end up with better lives, producing more without as much hassle.

I. INTRODUCTION

The agriculture sector provides about 50% of India's employment and is an increasingly important aspect of India's economy. Nevertheless, India's level of agricultural machinery utilization is comparatively lower than that found in developed nations. Many farmers cannot embrace mechanised farming because of high cost of farm machinery, limited access to farm that are mechanically farmed. To improve access to agriculture machinery the Government of India has established 75,000 Custom Hiring Centers (CHC) through which farmers are able to rent agricultural machines at subsidized rates. However, this is not addressing the issues of farmers experiencing high idle time due to CHC's not providing digital access to machines or an efficient system for booking machines and, also having in-sufficient trained operators to operate the machinery. Research indicates that on average, 40% of machinery is unused during the growing season..Simultaneously, machinery rental sectors based on ride-sharing type concepts have also had difficulty with costs attributed to logistics related to distance travelled by machines from one location to another. An additional challenge that currently exists in these sectors is what is known as the 'operator gap', whereby there is machinery available for rent but insufficiently trained people available to operate that machinery. This paper provides a proposed solution to address both of these challenges through the implementation of a hybrid aggregator solution called Operat-o-Farm that links to-gether government-operated Custom Hire Companies (CHCs), private machinery owners, and independent operators (Hertz). The Operat-o-Farm system seeks to improve the utilization of machinery by providing the following features: hyper-local discovery of available machinery, predictive analysis of expected future demand for the machines and a marketplace of potential operators utilizing a gig economy model.

Furthermore, This platform integrates with an e-RUPI based subsidy redemption mechanism that provides farmers access to subsidized service in a way that is easy and easy to use. The proposed system will help eliminate machine idle time, provide better access to farm equipment, and facilitate faster/easier agricultural operations.

II. BACKGROUND

Agriculture is really big in India's economy, especially for all those people in rural areas who depend on it for their living. A lot of farmers out there are small scale, and they struggle with getting the right tools because stuff like tractors and harvesters cost way too much.I believe that using machines would be an advantage because they can speed up production and reduce a lot of manual labor. But purchasing equipment isn't possible for most farmers. Therefore, to address this issue, there are custom hire centres and renting options allowing farmers to rent equipment when needed instead of buying all their own. This solution helps improve accessibility without all the costs upfront. However, problems do exist that make renting equipment more complicated, including farmers being unaware of what equipment is available or how far away it is; long wait times to book equipment; and insufficient operators with the skill set required to properly operate the equipment. Digital technology could provide a

solution to these challenges. There are now applications or platforms that will connect all the relevant parties (i.e., farmers, equipment owners/operators) in one central location. This could reduce lead-time on renting agricultural equipment and provide easier access for farmers to rent equipment. It appears that there is an opportunity for some type of integrated system to connect all the parties I mentioned, but I am not sure how feasible it will be. The main challenges of awareness and availability of rental equipment are ongoing; as such, the entire process is somewhat messy.

III. OBJECTIVE

The major objective of the present research is to develop an efficient web-based system for the effective management of agricultural machinery rental services in the rural regions of Maharashtra. The proposed system is designed to facilitate process of accessing agricultural equipment by bringing farm-ers, owners of agricultural equipment and operators together through a unified platform. The platform enables farmers to access agricultural equipment through centralized system and book the equipment as per their farming requirements. The other major objective of the present research is to enhance the transparency and efficiency of the agricultural equipment rental services. The system is designed to show the availability of agricultural equipment and estimate the rental costs as well as track the status of the booking process. This helps to avoid the uncertainties and delays experienced by the farmers while accessing agricultural equipment during critical farming seasons. Also, the study seeks to develop a specific interface for the owners of machinery, such that they can register their equipment and track the rentals in a structured manner. This aspect of the system can increase the usage of the equipment and can attract the participation of private owners as well as government- sponsored Custom Hiring Centres. The study also seeks to promote the cause of digital inclusiveness among the farmers in the rural areas through the development of a user-friendly interface for the website. This can increase the efficiency of farming activities and reduce the costs of operation for the farmers.

IV. LITERATURE REVIEW

A. Inefficiency of Existing Custom Hiring Centres (CHCs)

Singh and Vahoniya (2025) in their extensive research on Custom Hiring Centres in India, have identified the inefficiency of the existing Custom Hiring Centres. According to their research, the existing Custom Hiring Centres have the required infrastructure, but there is a problem of digital visibility, which results in “information asymmetry.” The farmers are not aware of the availability of the required machinery and where it can be hired. As a result, there is artificial scarcity of the required resources, which are already available. In addition to the above, Ganavi et al. (2024) have identified the inefficiency of the existing Custom Hiring Centres, which results in a delay of 15-20 days in the peak season. The inefficiency of the existing Custom Hiring Centres is the major problem because it has a static structure and does not have real-time inventory. However, the proposed Operat-o-Farm system

has the advantage of a hybrid aggregator platform, which includes government as well as private fleets.

B. Limitations of “Uber-for-Tractors” Models

There were digital platforms that tried to emulate the taxi model of the “Uber-for-Tractors” concept of rental services. In the study by Daum et al. (2021), it was noted that the taxi model is not effective for the rental of farming equipment. Farm machines like tractors and harvesters are costly to transport over long distances. The cost of transporting the machines is usually referred to as “deadhead costs.” The inefficiency of the taxi model is the reason why most of the private rental startups failed. The proposed Operat-o-Farm platform addresses the inefficiency of the taxi model by using the hyper local geofencing method. The method gives priority to the machines within a small distance of the farmer who requests the machine.

C. The Operator Gap in Agricultural Mechanization

Another challenge identified in the mechanization of agriculture was the lack of skilled machine operators. Brownstone (2025) observed that availability of machinery does not by itself guarantee improved agricultural productivity because many farmers lack the trained manpower to operate sophisticated machines used in agriculture. This assertion is supported by the fact that, according to FICCI reports (2025), the agricultural sector has a workforce skill gap of almost 30%. In order to resolve the operator gap, the proposed system will comprise a platform where machine operators can register their skills, enabling them to find work. This will create a separate market for machine operators from the machine ownership market, allowing farmers to hire the services of the operators separately.

D. Digital Subsidy Systems and e-RUPI

Recent developments in the digital financial system have introduced a new form of government subsidy systems. The NIC Odisha Report (2025) has documented the successful pilot project implementation of e-RUPI vouchers for subsidizing agricultural equipment. The e-RUPI vouchers enable the direct receipt of government subsidies by the farmer without the need to fill out complicated paperwork. Expanding on e-RUPI voucher idea Operat-o-Farm platform has incorporated the facility of e-RUPI vouchers within platform to enable the direct application of government subsidies to the farmer while renting the machinery.

V. PROBLEM STATEMENT

There are a number of issues that farmers in the rural regions face when it comes to accessing agricultural machines to carry out farming activities. First and foremost, purchasing machines such as tractors, harvesters, and sprayers requires a significant amount of investment, which is not within the economic power of many farmers. Although there are rental services and initiatives such as Custom Hiring Centres (CHCs) from the government to provide machines to the farming community, most of them are not fully digitalized and are carried out offline. This creates a number of

issues for the farming fraternity as accessing machines is not an easy affair. There is no clear system of communication between the farming fraternity and the owners of the machines, and most of the time, the farming fraternity is not aware of the availability of machines in their regions. In addition, existing platforms do not effectively integrate the machinery providers, the operators, and the subsidy mechanisms into a single platform. As a result, there is a need to develop a unified digital platform to make the process of renting agricultural machinery easier. A smart agricultural machinery rental system has the potential to offer real-time information regarding the availability of the machinery, make the booking process easier, enhance transparency in the pricing of the machinery, and enhance the level of communication between the farmer and the service provider.

VI. METHODOLOGY

The proposed system, namely Operat-o-Farm, will be based on a structured methodology that will involve data collection, system design, algorithm development, platform implementation, and system evaluation. The main objective of using a structured methodology is to ensure that a highly efficient digital platform is created that will connect farmers, machinery providers, and machine operators in a manner that is accessible, minimizes idle machine hours, and ensures transparent subsidy distribution.

In the first phase of developing the system, relevant data will be collected. This will include various types of data, such as information related to machinery that is available with Custom Hiring Centres (CHCs), information available with individual machinery owners, operator availability, and farmer requests to hire machinery. Other relevant information will also be taken into consideration. This will include location, type of crops, and seasonal patterns. The data will be used to understand machinery required and machinery available in different locations. In the second phase data collected is processed and organized in system database. Data cleaning and validation are done to ensure accuracy and consistency of data. Information about the availability of the machinery, skills of the operator, rental costs, and location is structured to enable efficient access to the data by the platform.

In the third phase, the hybrid aggregation mechanism is used to integrate the government CHCs and the private providers of the machinery on a single platform. The system identifies the available machinery within a specified radius from the farmer's location. A geo-fencing priority algorithm is used to reduce the distance of travel to the farmer's location, thus reducing the cost of logistics. The machines are ranked based on their availability, distance to the farmer's location, and the estimated cost of travel before they are presented to the farmer.

In the fourth phase, the operator management module is incorporated to mitigate the scarcity of skilled machine operators. The operator can register his or her profile, add his or her work experience and skills, and receive service requests through the platform. A ranking system will rank the operator based on ratings, work experience,

and the number of tasks completed. This ensures that reliable and skilled machine operators are assigned to operate machines.

The system has been enhanced to incorporate the digital subsidy mechanism through the e-RUPI vouchers. The eligible farmer can upload his or her land records, which are verified through the platform. Once land records are verified platform will generate a secure digital voucher which can be redeemed while booking machinery services.

In the implementation phase the platform is built as web based system with support from the cloud infrastructure. The interface would enable farmers to search for the equipment, compare prices, and book the services, while the vendors would be able to manage the equipment. The system would also enable the operators to receive notifications for jobs and accept the assignments. This integrated approach facilitates communication among all the actors. The performance of the proposed system is assessed based on the efficiency of the system during operation, the efficiency of the machinery used, and the accessibility of the services provided by the system. The performance metrics are the time taken to book the services, the idle time of the machinery, and the success of the services provided by the system, which are used to assess the effectiveness of the proposed system in enhancing the availability of agricultural machinery services.

VII. SYSTEM ARCHITECTURE

The Operat-o-Farm system uses an integrated architecture that brings together farmers, those providing agricultural machines, operators, and government subsidy services through a unified platform. The system can be accessed by a farmer through a mobile/web interface to search and request agricultural machines according to their requirements and locations. Once a request is made on the platform, the system retrieves agricultural machines from both government Custom Hiring Centres (CHCs) and other owners of agricultural machines. The system uses a location-based matching system to find agricultural machines within a specific geographical area and ranks them according to their availability and travel distance. If a skilled operator is required to run the agricultural machines, the system uses the Operator Module to notify and assign the task to the operators according to their availability.

The system also checks the farmer's eligibility for a government subsidy and generates an e-RUPI token.

After the agricultural machines are used for the purpose required by the farmer, the service provider makes use of the e-RUPI token to record the transaction and make payments via the system. This architectural model combines services provided by agricultural machines, operators and government subsidies to provide holistic service for agricultural machine rental.

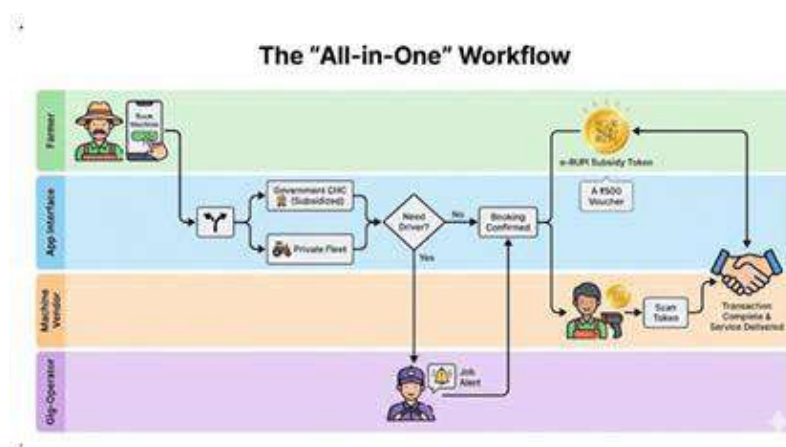


Fig.1. All-in-One Workflow of the Proposed Operat-o-Farm System

VIII. CONCLUSION

This paper introduced a hybrid digital platform called Operat-o-Farm, aiming to facilitate access to agricultural machines for rural farmers. The suggested system brings together the services of Custom Hiring Centres (CHCs) offered by the government, machinery suppliers from the private sector, and individual operators on a single platform. This system addresses some of the major issues affecting agricultural mechanization, unavailability of machines, inefficient booking system, unavailability of skilled operators, and others.

It also has various features such as machine location discovery, gig operator marketplace, e-RUPI subsidy feature, which helps in providing support to farmers by the government. The various features are directed towards ensuring that idle times are minimized for the machine, costs are reduced, and transparency is ensured for machine rental. The system also helps in fast communication between farmers and service providers, which ensures timely access for the farmers during the critical farming period.

It can be concluded that the proposed solution has clearly shown the benefits of using the digital platform for improving the service provided for the farmers and enhancing the productivity of the farming sector in the future. The system can be further enhanced in the future by adding various functionalities such as the implementation of predictive analytics for forecasting the demand for the machines and using satellite data for enhancing the decision-support system for the farmers.

REFERENCES

- [1] M. Singh and D. R. Vahoniya, "Custom Hiring Centers in Indian Agriculture: A Comprehensive Review," *Asian Journal of Current Research*, vol. 10, no. 4, pp. 23–34, 2025.

-
-
- [2] N. R. Ganavi et al., “Impact of Custom Hiring Centers on Cost, Profitability, and Efficiency,” *Journal of Scientific Research and Reports*, vol. 30, no. 5, pp. 580–587, 2024.
 - [3] T. Daum, R. Villano, and S. R. Bharadwaj, “Uber for tractors? Opportunities and challenges of digital tools for tractor hire in India,” *World Development*, vol. 144, 2021.
 - [4] R. S. P. Singh, “Impact of Agricultural Mechanization on Production and Productivity,” *Journal of Agricultural Engineering*, vol. 54, no. 2, 2024.
 - [5] S. Brownstone, “Labor Market Effects of Agricultural Mechanization: Experimental Evidence from India,” *Job Market Paper*, Department of Economics, 2025.
 - [6] Agtivation, “Forecasting Agricultural Equipment Demand With Predictive Analytics,” *Agtivation Industry Report*, 2025.
 - [7] Meegle, “Predictive Analytics for Agricultural Forecasting Tools,” *Meegle Tech Review*, 2025.
 - [8] FICCI and Grant Thornton, “Transforming Agriculture Through Mechanisation,” *FICCI Knowledge Paper*, 2025.
 - [9] S. Balasundram et al., “Digitalization of Agriculture for Sustainable Crop Production: A Use-Case Review,” *Frontiers in Environmental Science*, 2024.
 - [10] GKToday, “e-RUPI: Implementation and Benefits in Welfare Schemes,” *General Knowledge Today*, Oct. 2025.
 - [11] NIC Odisha, “e-RUPI: Inauguration at Farm Mechanization Krushi Mela,” *National Informatics Centre Report*, March 2025.
 - [12] C. Das and S. B. Patil, “Perception vs. Performance of Custom Hiring Centres,” *International Journal of Environment and Climate Change*, vol. 14, no. 9, 2024.

PRIVACY GUARD WEBSITE: A WEB-BASED SYSTEM FOR DETECTING AND PREVENTING DATA PRIVACY RISKS IN ONLINE APPLICATIONS

Dr. Pratibha Deshmukh¹, Shivraj Mahatme² and Anjali Rathod³

¹Project Guide, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

^{2,3} Student, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

ABSTRACT

Mobile applications often request access to sensitive user data such as location, camera, and contacts, raising privacy concerns. Unauthorized access and third-party tracking can lead to data misuse.

This project introduces PrivacyGuard, a web-based tool that evaluates privacy risks of mobile applications using a rule-based scoring model. It analyzes user-uploaded data (CSV/JSON) and classifies apps into High, Medium, or Low risk based on permissions and trackers.

Built using Spring Boot (backend) and HTML, CSS, JavaScript, and Thymeleaf (frontend), the system provides visual insights like charts for better understanding. The tool performs real-time analysis with minimal processing time, helping users make informed privacy decisions.

I. INTRODUCTION

Today's digital world sees mobile applications incorporated into everyone's daily life – enabling communications; work; entertainment; and access to various forms of online services. However, the rapid proliferation of mobile applications creates major issues related to the privacy and security of users' personal information. Most mobile apps require users to provide access to sensitive information (e.g., location, camera, microphone, contacts, storage), but many times they provide no real justification for needing access to that particular sensitive piece of information. Unrestricted access to users' personal information can create major legal issues for the developer, and significant liability issues for the developer's company if a user's personal information is compromised. can lead to privacy risks, such as data leaks, unauthorized use of data, and tracking by third parties.

Studies conducted recently reveal that users give permission to apps without fully realising the implications of this action. The increasing usage of smartphones in developing countries, such as India, creates a growing number of people using mobile applications for day-to-day activities, with low levels of understanding about the risks associated with providing permission. The combination of complexity surrounding

permissions and the lack of understanding creates an increasing disparity between the expectations of the user and the way their personal data is actually managed.

Several research projects have looked at ways to analyze app permissions and spot potential privacy risks. Current methods focus on static permission checks, rules for evaluation, and tracking detection. However, many of these systems do not have user-friendly interfaces and fail to explain risks clearly. Also, the lack of effective visualization tools makes it hard for non-technical users to grasp privacy risks.

Visualizing data and user-centred design play a major role in recent developments in the area of privacy analysis. Using interactive dashboards/graphs assists users with understanding privacy related data more effectively. Overall, this progression demonstrates a need for an effective, accurate way of evaluating a user's privacy risk while also providing an easy-to-understand presentation of those findings.

PrivacyGuard aims to address these issues by providing a web-based application to evaluate the privacy risks associated with mobile app usage via mobile app permissions. With the PGE app, users upload a mobile app permission CSV or JSON file and their corresponding privacy risks (based on sensitive permission types and tracker detection) will be evaluated based on adherence to a defined ruleset and classified as either high, medium, or low-risk categories. The resulting evaluation level of a given user-uploaded mobile app permission file will be visually displayed through clearly defined visual representations of the results of each evaluation level, including but not limited to donut charts and summaries of app permission data to assist users with making educated decisions regarding their use of mobile applications their digital privacy.

A. Motivation

The primary goal of building PrivacyGuard is based on a number of recent research findings::

- Users are typically not aware of how app permissions affect their security/privacy of personal data.
- Existing resources do not clearly define the privacy risk associated with permission of use for mobile applications.
- A better and easier way to evaluate the use of app permissions and determine if using a particular app will result in a negative outcome regarding the user's right to privacy is necessary.
- As the need for data privacy is growing, resources that allow users to make informed decisions, based on actual data, in an ever-increasingly digitally-driven world, will be critical.

B. Objectives

The intent of the proposed site is three-fold:

-
-
1. To develop a rule-based risk scoring model that categorizes applications as High, Medium, or Low privacy risks.
 2. To evaluate application data provided in CSV or JSON format and perform real-time privacy risk assessments.
 3. To identify sensitive permissions and tracking mechanisms that contribute to privacy risks.
 4. To design an engaging user interface that visualizes privacy insights through charts and app summaries for better understanding by users.

II. RELATED WORK

Researchers have conducted several studies addressing mobile app privacy and protecting user data through permission analysis, rule-based models and security frameworks. The goal of this type of research is to resolve growing issues with using someone's data improperly and gaining undue access to that information.

A. Mobile Application Privacy Analysis

More research has focused on studying the granting of permissions by mobile applications in order to determine where privacy could be compromised. It has been demonstrated that a large number of mobile applications make requests for access to information that are not required in order to carry out their function. This unnecessary request for access to data can increase the chances for data leakage. Static permission analysis approaches use static behavior analysis to identify privacy-defining behavior of mobile applications, while other rule-based approaches use intrinsic metrics associated with privacy-sensitive permissions to assign risk scores. The scoring of risk can be used to categorize mobile applications into several different levels of risk.

B. Permission-Based Risk Evaluation and Tracker Detection

The need to connect permission analysis with tracing identifier techniques to enhance privacy risk assessment has become the focus of more recent work. Third-party tracking libraries such as analytic toolkits and ad toolkits form a significant portion of the user data and profiling that occurs through data collection techniques. Permission weighting, risk scoring models, and tracking libraries are all examples of techniques developed to create enhanced privacy risk assessments. These methods can help to provide a better level of risk classification accuracy, provide an opportunity to discover hidden data sharing through applications, and result in enhanced data-sharing identification in applications.

C. Visualization and User-Centric Privacy Systems

Recent research has demonstrated that visualization and user-centered design are vital in raising user awareness around privacy. There is an increasing trend towards using interactive dashboards, graphical displays, and visual analytics tools to make complex privacy information more easily understood. By presenting users with risk levels to help them make informed decisions on how to use an application, users will

have a greater understanding of the potential risks they may be exposing themselves to as they utilize their devices. Combining visualization techniques with back-end analysis has also proven to be a successful method for improving the usability and accessibility of privacy-oriented systems, particularly for non- technical users..

These studies highlight the increasing importance of privacy- aware systems that blend permission analysis, risk evaluation, and clear visualization. The PrivacyGuard Website builds on these ideas by offering a web-based platform that combines rule-based risk scoring, tracker detection, and inter- active visualizations for a thorough and user-friendly privacy analysis solution.

III. PROBLEM STATEMENT

With mobile applications becoming increasingly popular, the importance of user privacy when it comes to protecting private information is essential. The majority of mobile applications request access to sensitive types of information like location, camera, contact lists, voice recording, and external storage. Users frequently grant this access to their private information without fully comprehending what it entails. As a result, users can be affected by risks such as data leaks, unauthorised access, and third-party tracking of their activities. Users aren't aware of all these potential risks, which creates a gap between what users believe will happen to their private information (i.e. remain secure) and what actually happens (i.e. may be shared with others).

Currently, the primary means by which users evaluate the potential for their private information to be accessed by a mobile application is by reviewing the list of permissions requested by the application through the app store where the application has been obtained. However, while this method allows users to know the permissions requested, it does not provide users with sufficient information to determine the risk associated with each permission in regard to the impact of the permission on their privacy. As well, manually reviewing the

PROPOSED PRIVACYGUARD SYSTEM

A. System Architecture

The PrivacyGuard system is a flexible and scalable webbased system comprising various modules to provide data processing, risk analysis based on rule-sets, and visualization capabilities. The overall system architecture consists of several layers:

- 1) Data Input Layer User-provided application data can be uploaded through this layer in either CSV or JSON format, and will contain information on the application name, package name, permissions and any optional tracker data.
- 2) Data Preprocessing Layer This layer will verify, clean, and convert permissions into an analyzable, structured format.

3) Risk Analysis Layer A rule-based scoring model is implemented in this layer to assign scores (via weights) to permission sets based on their sensitivity and to check for third-party trackers.

4) Application and User Interface Layer A browserbased application or web site will serve as the vehicle for presenting results; results will be presented as charts and application summary reports to assist the user in comprehending the information above.

B. Functional Modules

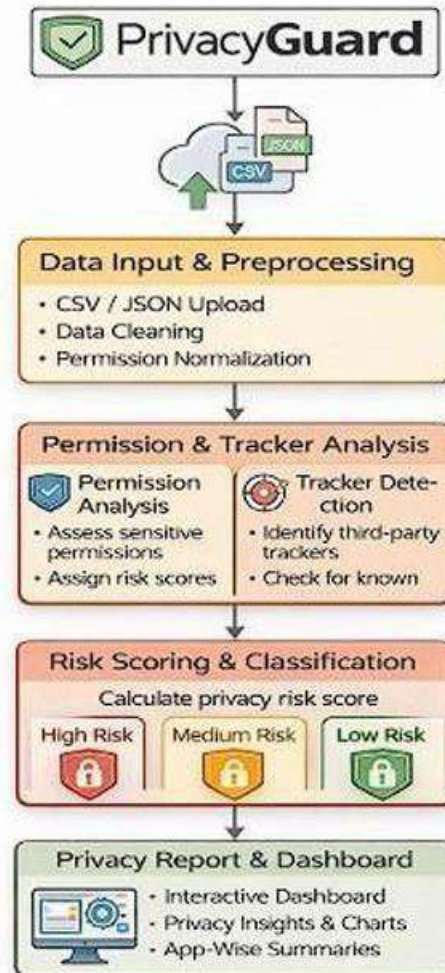
The enabling functionalities for the proposed system are as follows:

- Data Preprocessing Module Validates uploaded files, cleans the data, normalizes permission formats, and re- moves inconsistencies.
- Permission Analysis Module analyzes the permissions based on sensitivity level, assigns an appropriate classification level to each permission and establishes a minimum threshold of sensitivity for each permission type.
- Risk Scoring Module calculates a risk score associated with each permission type through a set of pre-defined rules, by applying weight to each permission and by penalizing for any tracking devices (i.e., third-party libraries, Software Development Kits (SDKs), etc.) that are present or that may be present.
- Risk Classification Module provides an overall classification for each application based on its cumulative risk scores that fall into one of three classifications (High, Medium, Low) as established in rule 2.
- Tracker Detection Module detect any third-party tracking libraries (e.g. AdMob, Facebook SDK, Firebase, etc.) that are included with the application..
- Visualization Module presents the user's privacy risk as a summary in the form of bar charts (i.e., donut charts) and summarizes all applications in regards to their privacy risk up to this point.

IV. WORKING

The PrivacyGuard system starts by collecting data from users. This data is about the applications that are installed. It includes the name of the application the package name, what

- The first part of an app's score will be based on how much access to your information the app needs. Apps with more than 3 or 4 permissions will have a higher score than apps with fewer permissions.
- Once the permissions for each app have been checked, then the system refers to a list of known tracking libraries.



V. DATASET DESCRIPTION

A. A. User-Uploaded Application Dataset

The permissions dataset assigns weightings to permissions based on how sensitive they are in order to create a privacy risk score.

B. B. Permission Dataset

The permissions dataset assigns weightings to permissions based on how sensitive they are in order to create a privacy risk score.

C. C. Tracker Dataset

A dataset containing a list of known third-party tracking applications. Examples of third-party tracker applications include Firebase and AdMob. The tracker dataset is used to identify any tracking activities.

D. D. Output Dataset

The output dataset consists of privacy risk scores, classification levels, and information regarding any detected permissions or trackers. This dataset may be used for visualization.

- High Risk (Score 15)
- Medium Risk (Score 7–14)
- Low Risk (Score 0–6)

IX. EVALUATION APPROACH

In order to evaluate the PrivacyGuard system, we will conduct a rule-based analysis using the following method: 1) Classify the risk associated with the use of the data:

TABLE I: Dataset Description

Type	Format	Description
User Data	CSV/JSON	App name, package, permissions
Permissions	Internal	Weight-based risk values
Trackers	Internal	Detects Firebase, AdMob, etc.
Output	Generated	Risk score (High/Med/Low)

VI. DATA PREPROCESSING

A. Data Cleaning

- Validation of uploaded CSV/JSON files & Handling Missing Values.
- Removal of duplicate/inconsistent application records.

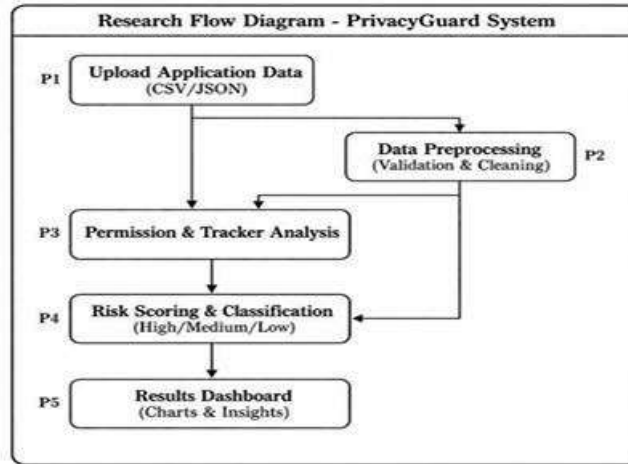
Data Processing

- Normalization of permission formats for consistent analysis.
- Mapping permissions & trackers to known risk data setsRISK

B. Risk Classification

Permission based Risk Scoring and Accurate Tracker Detection. 2) Visually represent the distribution (High/Medium/Low) of the risks identified above.

END-TO-END WORKFLOW DIAGRAM



The first step in the PrivacyGuard workflow is the user uploaded application data in either CSV or JSON format. After that, preprocessing and the determination of needed permissions will occur. Using a rule based model of risk scoring and tracker identification, the applications will then be placed into categories,

i.e. high, medium, low risk categories. Then, after this process has been completed, the overall results of the process will be presented on an interactive dashboard for easy analysis.

EVALUATION MODEL

A. Risk Scoring Based on Rules

The PrivacyGuard system assesses application privacy risks using a rule-based methodology:

- Tracker Detection Mechanism
- Permission Weighting Model
- Risk Classification (High, Medium, Low)
- Tracker Detection Accuracy
- System Response Time
- Visualization Clarity and Usability

X. DISCUSSION

Experiments set forth in our results demonstrate that the Childhood Obesity Prediction System, which utilizes machine learning techniques while incorporating many lifestyle, demographic, and anthropometric variables, outperforms any other System to date. In comparing the various predictive models (for example: Random

Forest, XGBoost, Decision Tree), it was found that ensemble models provided greater predictive accuracy and improved performance on a per-class basis compared to non-ensemble models.

Data pre-processing and feature engineering were important in developing model robustness by reducing noise from missing or erroneous data, as well as incorporating lifestyle elements, including physical activity, diet, screen time, and sleep patterns, which significantly improved prediction accuracy relative to the traditional BMI-based method of evaluating children for overweight and obesity.

The modular nature of the System and Streamlit Dashboard

will allow users to easily interact with the System and provide interpretability and scalability. By focusing on actionable insights rather than just predictions about childhood obesity, this system has practical applications to schools and pediatric clinics, particularly in the context of India.

XI. RESTRICTIONS

- The main limitations of the system are as follows:

User-uploaded application data must be both accurate and complete for this system's operation. Like all rule-based systems, it is unable to capture all of the complex privacy risks that are captured by more complex machine learning models. The first and most important factor in the operation of this system is the use of tracker datasets as well as the use of pre-defined permission weights. research flow diagram) starts with user data upload and preprocessing, followed by permissions and tracking analysis. The workflow will display an interactive dashboard with insights and visualizations of privacy based on rule-based classifications/risk scoring.

EVALUATION METRICS

The performance of the proposed PrivacyGuard system is evaluated using these metrics:

- Permission-Based Risk Score

CONCLUSION

This research presented a rule-based method of assessing mobile application privacy risks through the analysis of the permissions and tracker data. The privacy risk evaluation system utilizes data preprocessing, permission and tracker assessment, and risk scoring to facilitate the evaluation of and obtain a risk score for the privacy risks associated with an application

The PrivacyGuard tool provides real-time analysis of data users upload and an interactive environment where users are able to view and analyze the privacy risks associated with particular mobile applications based on the permissions requested by that application and the associated tracker used by the application.

APPENDIX

APPENDIX A: ALGORITHMIC SYNOPSIS OF THE SUGGESTED SYSTEM

The suggested PrivacyGuard system implements an organized algorithmic workflow to assist users throughout the process of obtaining an understanding of their privacy risk through the evaluation of Mobile & Web app permissions. In all cases, user-uploaded application data must first be compiled and preprocessed (e.g., normalizing permissions, eliminating duplicates, and verifying data); thereafter, the system performs a permission analysis to identify those permissions deemed sensitive and any third-party trackers associated with the application that may pose a risk to the user's privacy.

The processed application data is subsequently evaluated for risk using a rule-based methodology that assigns predefined weights to permissions based upon their respective sensitivity, and additional penalties to third-party tracking systems identified by privacy analysis. Each application is organized into a risk category of either high, medium, or low risk for privacy based upon the consolidated risk score they accrued from both permissions and third-party trackers.

An interactive web-based dashboard is delivered through the system in which users can view the findings of the analysis conducted about their privacy risks and understand the behaviour of applications on a continual basis in real time. In doing so, it produces a higher degree of awareness of the privacy risks posed by their applications, as well as supporting better-informed choices regarding both data privacy and use of an application.

REFERENCES

- [1] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in Proc. ACM CCS, 2011.
- [2] K. W. Y. Au, Y. F. Zhou, Z. Huang, and D. Lie, "PScout: analyzing the Android permission specification," in Proc. ACM CCS, 2012.
- [3] S. Arzt, S. Rasthofer, and E. Bodden, "FlowDroid: Precise taint analysis for Android apps," in Proc. PLDI, 2014.
- [4] M. Backes, S. Bugiel, and E. Derr, "Reliable third-party library detection in Android," in Proc. ACM CCS, 2016.
- [5] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in IEEE S&P, 2012.
- [6] A. Shabtai, Y. Fledel, and Y. Elovici, "Securing Android-powered mobile devices using machine learning," IEEE Security & Privacy, 2010.
- [7] D. Geneiatakis et al., "A permission verification approach for Android apps," Computers & Security, 2015.

-
-
- [8] A. R. Khunt and P. Prabu, "Analysis of Android permission system based on user activities," *Journal of Computer Science*, 2018.
- [9] J. M. Arif et al., "Static analysis for Android permission-based malware detection," *IEEE Access*, 2021.
- [10] T. Tu et al., "Analysis of privacy policy and permission usage consistency," *Applied Intelligence*, 2024.
- [11] M. Liu and Q. Wang, "Android privacy permission analysis under big data environment," *MATEC Web Conf.*, 2024.
- [12] A. Alkinoon et al., "Analysis of evolving permission usage in Android apps," *MDPI Electronics*, 2025.
- [13] Google, "Android Permission Model," Available:
<https://developer.android.com/guide/topics/permissions>

ENHANCING ACADEMIC DECISION-MAKING THROUGH PCA, SENTIMENT-ANALYSIS AND TOPIC-BASED ANALYSIS OF RATING- BASED STUDENT FEEDBACK

Vedant Pawar¹ and Dr. Priya Chandran²

¹Department of MCA, Bharti Vidyapeeth's Institute of Management and Information
Technology, Navi Mumbai, India

²Department of MCA, Associate Professor, Bharti Vidyapeeth's Institute of
Management and Information Technology, Navi Mumbai, India

ABSTRACT

This paper talks, about a framework that helps analyze student evaluation data. It does this to support decision- making in schools. Traditional evaluation systems use numbers. These numbers are usually averages. They miss out on what students really think. Also not all students participate. So the numbers can be misleading. The EduSent framework tries to fix these problems. It looks at both numbers and attendance. This way it gives a picture. The outcomes are more reliable and easier to understand. The framework helps schools make decisions and it does this by giving them accurate information. EduSent makes student evaluation data more useful.

The system uses numbers and patterns to help figure out what students are saying. It also groups questions to make it easier to understand what students think about different teachers. The system looks at how students feel about things by checking the question words and rating they given. It uses a few methods, like TextBlob, VADER and a special kind of model to see how students really feel when they give feedback.

The Turkiye Student Evaluation dataset was used to see how well the new method works. It turns out that this new method gives ideas about what students think compared to just taking the average. The results also show that models using transformers are better, at understanding how people feel in situations. On the hand methods that use lists of words have a more neutral point of view. The Turkiye Student Evaluation dataset really helps to see that the new method is an improvement.

Index Terms—Educational Analytics, Student Feedback Anal- ysis, K-Means Clustering, Principal Component Analysis, Data Mining in Education, TextBob, VADER, Transformer

I. INTRODUCTION

Student evaluation of teaching(SET) make sure the quality of education is good and Universities use forms with questions that have answers like strongly agree or strongly disagree to see how well the teachers are doing their job how well they deliver the course and if the students are happy or something get undermine when delivering. These evaluations are really important, for deciding if the teachers are doing a job if the courses need to be improved and for making big decisions at the

university about student evaluation of teaching. Student evaluation of teaching helps the university to know what they are doing well and what they need to change.

Despite their widespread adoption, traditional evaluation systems face several limitations. Most existing approaches depend on simple statistical aggregation techniques, such as mean scores, which often fail to capture variability and patterns in student responses. As a result, important nuances in feedback are overlooked, leading to incomplete or potentially misleading interpretations of teaching performance. Furthermore, these systems do not account for differences in student engagement levels. Feedback from students with low attendance may influence evaluation outcomes as much as feedback from actively participating students, introducing bias and reducing the reliability of evaluation results.

With growing of educational data mining, there has been a emphasis on developing data-driven approaches for analyzing student feedback. These approaches cover the hidden patterns in evaluation data, identify meaningful group of responses, and improve the understanding of teaching assessments [4]. Previous Studies have shown the importance of combining structured evaluation data with analytical techniques to enhance feedback analysis and support decision-making processes in higher education. [8].

To solve these problems we suggest EduSent. It is a framework that helps us understand student evaluation data better. EduSent combines attendance information with machine learning methods. [1], [2]. The framework works with rating data cleans and prepares it. Then uses methods, like clustering and dimensionality reduction. These methods help find patterns in what students say about their teachers. The framework also groups questions together. This helps us see how well teachers are doing in areas. EduSent makes it easier to understand student feedback. It does this by using attendance information and advanced data techniques. This way we can get more out of student evaluations.

In addition to that studies on sentiment analysis and opinion mining have shown that advanced analytical methods can really help us understand data better. [1], [2]. However, many of these methods depend a lot on text feedback, which's often not available or limited in structured evaluation datasets. We need frameworks that can analyze data effectively and still give us useful insights, from educational data. These frameworks should help us get insights without relying on feedback. So, we can still learn a lot from data.

In addition to structured analysis, this study understand a comparative sentiment analysis component to provide an interpretative perspective on evaluation-related text. Multiple approaches, including TextBlob, VADER, and transformer-based models, are evaluated to understand differences in sentiment interpretation. This integration enables the framework to combine quantitative pattern analysis with qualitative insights, resulting in a more comprehensive evaluation of student feedback.

The proposed approach shifts the focus from simple score aggregation to a more comprehensive evaluation strategy that considers student engagement and response patterns. By combining attendance-weighted scoring with clustering and visualization techniques, the framework enables institutions to derive more reliable and actionable insights from student.

II. METHODOLOGY

The way we plan to do this is by following a step by step process for looking at student evaluation data and finding information. This system combines attendance records with statistics and other methods like grouping and simplifying data to make the evaluation system easier to understand and more trustworthy than the way of just looking at overall scores. Student evaluation data is what we are focusing on here. Student evaluation data is very important. These days people are using data to understand education and find patterns, in student feedback that are not easy to see. Student evaluation data is helping us to do this. [4], [8].

A. Dataset and Materials

The study uses the Turkiye Student Evaluation dataset. This dataset has than 5000 student evaluation records. Each record has 28 answers that rate parts of teaching. These answers are on a scale. They look at how well the teacher does their job. The record also has information about the teacher the subject they teach. If the students attended class. The Turkiye Student Evaluation dataset is easy to work with because it is structured. This makes it a good choice for looking at numbers and using computers to understand how well teachers do their job. People have used datasets like the Turkiye Student Evaluation dataset to see how well teachers teach and how students are engaged in class. The Turkiye Student Evaluation dataset is a tool, for this kind of study [8]

B. Data Preprocessing

If there are missing values they use mean methods to fill them in. This way the data stays good and accurate. They do this to make sure the ratings are fair and consistent, across all the features of the project. The rating values are very important so they make sure to handle them. Attendance values are extracted and normalized to a range between 0 and 1, forming the basis for engagement-aware weighting. This normalization ensures that attendance con tributes proportionally during evaluation score computation.

Unlike traditional feedback systems that rely on rich textual comments, the dataset used in this study primarily consists of

structured evaluation data. Therefore, preprocessing is focused on structured attributes, while limited semantic processing is applied to evaluation question labels to support interpretation of different teaching dimensions. This approach aligns with studies that show structured feedback analysis when textual data i.e. text is limited [1], [2].

C. Feature Engineering

Feature engineering plays a crucial role in enhancing the analytical capability of the framework. Several derived features are generated from the dataset to improve interpretability and support downstream analysis:

- **Mean Rating:** The average score computed across all evaluation questions for each student, representing overall perceived teaching effectiveness.
- **Attendance Weight:** A normalized value representing the level of student engagement, derived from attendance data.
- **Weighted Score:** An adjusted evaluation score that incorporates attendance influence, ensuring that responses from more engaged students have a greater impact.
- **Cluster Labels:** Group identifiers obtained through clustering analysis, representing different patterns of student evaluation behavior.
- **PCA Components:** Reduced-dimensional representations that capture dominant patterns in the evaluation data.

The weighted evaluation score is computed as:

$$R = w \cdot \frac{\sum_{i=1}^n Q_i}{n} \quad (1)$$

where w denotes the normalized attendance weight and Q_i represents individual Likert-scale responses. Incorporating engagement-aware weighting has been shown to improve the reliability of evaluation metrics in educational data analysis [4].

D. Proposed Framework

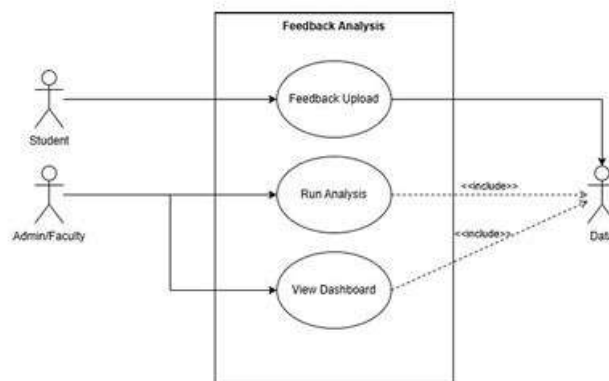


Fig.1. EduSent Use Case Diagram

The EduSent framework is made up of three parts that work together. The first part looks at data and it uses attendance scores to make the results more accurate.

The second part uses techniques like K-Means clustering and Principal Component Analysis to find patterns, in the data and show how things are related.

The third part tries to understand what the data through sentiment analysis by looking at how people feel about things and what topics are being talked about in the evaluations. This design makes sure that the EduSent framework looks at both numbers and what people think. It gets a complete picture of the EduSent data.

The EduSent framework is a tool that helps schools make sense of student feedback. It takes in data from student evaluations and turns it into useful information for teachers and administrators. The framework looks at student feedback in a way than usual. Of just using numbers it also considers how engaged students are. It does this by analyzing the feedback weighing it based on how much students participated and looking for patterns.

It starts by collecting student evaluation data, including ratings, on aspects of teaching and attendance information. These two pieces of information are used together. The ratings show how good a teacher is and attendance shows how engaged students are. By using both the system can get a picture of whats going on than just averaging the ratings. This helps it understand the feedback accurately. The EduSent framework provides a detailed understanding of student feed- back. This helps schools make decisions. The framework helps teachers and administrators understand what students really think. It considers student engagement. The framework uses student evaluation records. These records include ratings and attendance information. Ratings show teaching quality. Attendance shows student engagement. The system uses both to understand feedback.

After we get all the data we need to make sure it is clean and easy to use. We do this by making all the information the same and consistent. This step helps us get the data ready for analysis by taking out anything that does not make sense and making sure all the parts of the data are on the same scale. At the time we look at the questions we are trying to answer and group them together based on what they are really asking. This helps us understand the data better by putting all the information into simple categories. Doing it this way is something that other studies, in educational data mining have also found to be helpful. [8].

The next step focuses on feature engineering, where the framework takes meaningful keywords from raw inputs. In addition to computing average evaluation scores, the frame- work introduces attendance-weighted scoring to adjust the influence of individual responses. This mechanism addresses a critical limitation in traditional systems, where feedback from less engaged students may disproportionately affect outcomes. Incorporating engagement-aware weighting has been recog- nized as an important factor in improving the reliability of educational analytics [4].

To make the analysis better we use a framework that includes sentiment analysis with methods. Methods like TextBlob and VADER give us an understanding of the sentiment. However, they do not always capture the context well. Transformer-based models work better in this case. They can understand the context effectively. This is because they are based on improvements in natural language processing. The lexicon-based methods are okay. Transformer-based models are more accurate. The transformer-based models are really good, at understanding the nuances of language. This helps us get a detailed analysis. [10]. Comparative analysis of these models helps the framework to show differences in how they interpret sentiment and find biases in simpler methods. We can see variations in sentiment interpretation. Potential biases in methods are identified. Similar hybrid approaches have been tried in research to improve opinion mining, in educational settings. These approaches aim to enhance opinion mining. [5], [6].

The framework does more than just look at how people feel. It also uses a way of learning called learning to find patterns in the evaluation data that are not easy to see. The framework uses something called K-Means clustering to group feedback from students that's similar. This helps us find patterns in how students respond, like students who do very well students who do okay and students who do not do well. This way of grouping students is similar, to what people're doing now in education to find patterns in how students behave when they are learning. The framework is looking at student response patterns and evaluation data to understand how students are doing.

The framework uses K-Means clustering to look at student response patterns. The evaluation data is used to find patterns in how studentsre doing. This helps us understand student response patterns and evaluation data. [4].

To make sense of data with many parts we use Principal Component Analysis (PCA) to reduce the number of parts. This helps us see how different things are related to each other in a way. We can then visualize these relationships in a space that's easier to understand. This makes it easier to see how different groups are separated and how the data is organized. Principal Component Analysis (PCA) is really important, for helping educators understand the data. We need to be able to see the data in a way so we can make good decisions. Principal Component Analysis (PCA) helps us do that by giving us a picture of the data.

The dataset is mostly made up of evaluation data.. The framework gets its ideas from topic modeling and semantic analysis techniques. These techniques are used in studies, about feedback. The framework uses these techniques from educational feedback studies to do its job. The main thing is that the dataset has structured evaluation data and the frame- work uses techniques from educational feedback studies like topic modeling and semantic analysis. [3], [7]. The framework does not use a topic modeling system on the text. It uses a method, to group related words and give a better understanding of the evaluation dimensions. This way the framework

works with the type of data it is given. The framework uses this method to make sure it matches the data.

The results from all the parts that analyze things are put together in a way that's easy to understand. This is shown with pictures and charts. It helps the people, in charge understand the results and make changes to the way they teach. The new way of doing things combines looking at the numbers considering how engaged people are, understanding how people feel and grouping things together. This makes it a complete and flexible way to analyze education in a way.

The EduSent framework is really good because it helps us look at student feedback in a way. It brings together ways of evaluating things and new ways of analyzing data. This makes the EduSent framework a trustworthy and understandable tool for people who work in higher education and want to know what students are saying. The EduSent framework is very useful, for this purpose.

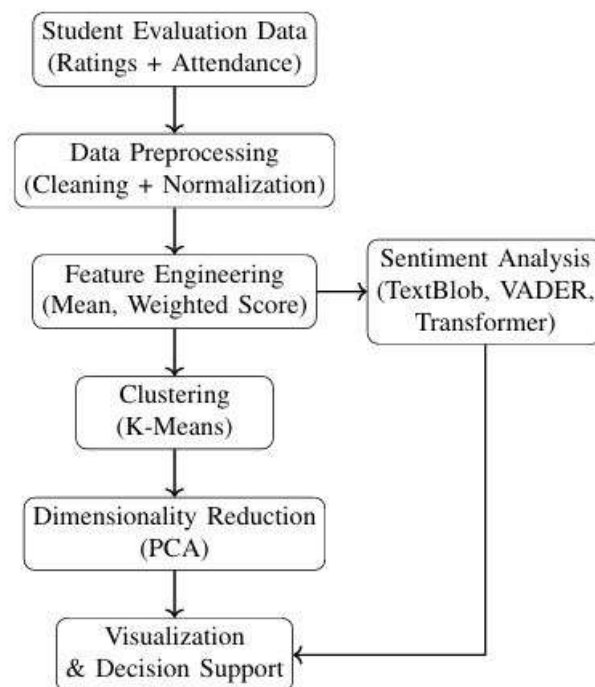


Fig.2. Proposed Framework of EduSent

III. RESULTS AND DISCUSSION

The experimental evaluation of the proposed EduSent framework was extended to include sentiment analysis using three different approaches: TextBlob, VADER, and a transformer-based model. This comparison enables a deeper understanding of how different modeling techniques interpret student feedback patterns.

The results show differences between the three models. The TextBlob model said that 75% of the feedback was neutral. It thought that 12.5% of the feedback was positive and 12.5% was negative. The VADER model was similar. It thought that 62.5% of the responses were neutral and 37.5% were positive. The VADER model did not think that any of the responses

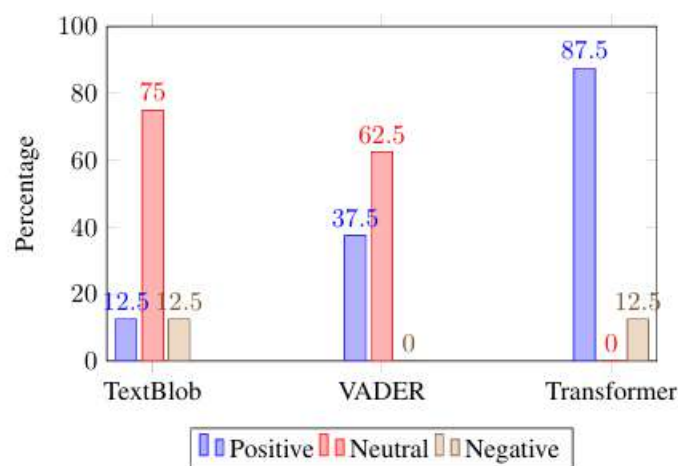


Fig.3. Comparison of Sentiment Distribution Across Models

were negative. This is what we expected to see. We already knew that models, like TextBlob and VADER tend to say that most feedback is neutral when they do not have information to work with. The TextBlob model and the VADER model are both examples of this. They are sentiment analysis models that often say that feedback is neutral. [1], [2].

In contrast the transformer-based model showed a different result. It said 87.5% of the feedback was good and 12.5% was bad. This means that transformer-based methods understand the context better than lexicon-based methods. They use embeddings that help them get the sentiment right. The transformer-based model works well because it looks at the text, not just individual words. It can tell when someone is being sarcastic or using idioms. This makes it better, at understanding how people really feel. [10]. Similar improvements in contextual sentiment understanding have been reported in recent deep learning-based educational analytics studies [5].

The difference in what models say shows that the old ways of figuring out how people feel from text do not work well when the text is short or has a structure. On the hand models that use transformers are better at saying what they think and are more sure of themselves which is why people like to use these new methods to understand what people think. This is especially true when it comes to understanding opinions and feelings, from text and people are starting to like these methods more and more. [6].

However we should note that the dataset in this study is mostly made up of evaluation data, not rich text feedback. This means that sentiment analysis is done on text inputs like evaluation descriptions, which might make the sentiment predictions less reliable. So we should see these results as how the models compare to each other not as final conclusions about sentiment. This is in line with what other studies on feedback have found. The limited text data used for sentiment analysis may impact the accuracy of the results. Therefore the findings should be viewed as a comparison of model performance, than absolute sentiment insights. [3].

We used some methods like sentiment analysis. We also used clustering and dimensionality reduction techniques on the dataset. The K-Means clustering method found three evaluation patterns. These patterns were for students who did well students who did okay and students who did not do well. Student behavior is often grouped in this way in educational data mining. This helps us find patterns in evaluation data that we might not have seen otherwise. We can use clustering to find these patterns in the evaluation data of students. Clustering is a method for educational data mining to find patterns, in evaluation data of the students. [4]. Principal Component Analysis or PCA helped us see these clusters clearly. It showed that they are well separated when we look at them in a way. We used PCA to make it easier to understand the data. The clusters are really distinct when you use PCA. This method helped us visualize the data better.

TABLE I COMPARISON OF SENTIMENT CLASSIFICATION ACROSS MODELS

Model	Positive (%)	Neutral (%)	Negative (%)
TextBlob	12.5	75.0	12.5
VADER	37.5	62.5	0.0
Transformer	87.5	0.0	12.5

So I looked at how attendance affects scores. I found out that there is a difference of about 10 to 15 percent, between the regular scores and the scores that take attendance into account. This shows that student engagement really matters when we are evaluating how well students are doing. The Student Engagement and the evaluation metrics are very important. This means that when we think about student engagement we can trust the feedback we get about how studentsre doing in their classes and the academic feedback interpretation of Student Engagement is more reliable. [8].

IV. CONCLUSION

This study introduces EduSent, a tool to help make sense of student feedback in universities. Traditional methods have some problems. EduSent tries to fix these by using a new ideas. It looks at attendance picks out details from the data and uses computer algorithms to get a better picture of how well teachers are doing. The goal is to make evaluations more accurate and easier to understand. EduSent works with

student evaluation data to provide a reliable assessment of teaching effectiveness. It helps to improve the interpretation of student evaluation data, in education.

The framework works with organized data. Uses K-Means to group similar things together. It also uses Principal Component Analysis (PCA) to make the data simpler. This helps find patterns in student feedback that are not easily seen.

The framework uses tools like TextBlob, VADER and some transformer models to do this. These tools give views on the text showing how each model understands the context differently. The framework looks at student feedback. Uses K-Means and PCA to find hidden patterns. It uses TextBlob,

VADER and transformer-based models to analyze the sentiment of the feedback. This helps understand the evaluation-related text. The K-Means and PCA help in identifying patterns. The TextBlob, VADER and transformer models provide insights into how people feel about things. The framework uses K-Means clustering and PCA for data analysis. It also uses TextBlob, VADER and transformer models for sentiment analysis.

The results show that attendance-weighted scoring makes evaluation outcomes more reliable. This is because it takes into account how engaged the students are.

When we look at the student responses we can see that they form groups. This helps us figure out which students are doing really well which ones are doing okay and which ones are not doing great.

We also used sentiment analysis to get information.. What we found out is that looking at groups of students and using attendance-weighted scoring is a better way to evaluate students when we have a lot of structured data from evaluations. The attendance-weighted scoring and clustering are more effective, for evaluation datasets especially when we have a lot of data.

The proposed framework is really good because it does more than just add up scores. It uses different ways to analyze things to make student feedback analysis better and easier to understand. This helps people make decisions about academics. The proposed framework also works well for groups of students, which is great, for schools that want to use modern ways to look at educational information. The proposed framework is a way to look at student feedback analysis.

Future work can focus on incorporating richer textual feedback, exploring advanced deep learning models, and developing real-time dashboards for continuous evaluation and monitoring of teaching effectiveness.

REFERENCES

- [1] Y. Shaik, P. Y. Shaik, and P. U. Yadav, "Sentiment analysis and opinion mining on educational data: A survey," arXiv preprint arXiv:2302.04359, 2023.

-
-
- [2] F. Dalipi, K. Zdravkova, and F. Ahlgren, "Sentiment analysis of students' feedback in MOOCs: A systematic literature review," *Frontiers in Artificial Intelligence*, vol. 4, p. 728708, 2021.
 - [3] J. Sun and L. Yan, "Using topic modeling to understand comments in student evaluations of teaching," *Discover Education*, vol. 1, no. 1, pp. 1–13, 2023.
 - [4] G. Fan and M. Feng, "Research on learning behavior patterns from the perspective of educational data mining," *Expert Systems with Applications*, vol. 222, p. 119675, 2024.
 - [5] M. Rahman and F. Hossain, "Deep learning-based sentiment analysis for course evaluation," *Education and Information Technologies*, vol. 27, pp. 895–915, 2022.
 - [6] M. Hasan, A. Noor, and M. A. Khan, "A hybrid model for opinion mining in academic text data," *Procedia Computer Science*, vol. 189, pp. 206–213, 2021.
 - [7] A. Barbosa and C. Lopes, "Improved topic modeling with domain-aware priors for educational feedback," *Journal of Educational Data Mining*, vol. 15, no. 1, pp. 45–60, 2023.
 - [8] T. H. Nguyen and D. T. Vo, "Feedback analytics in higher education: A case study," *International Journal of Educational Technology*, vol. 17, no. 2, pp. 113–125, 2020.
 - [9] D. M. Blei, A. Y. Ng, and M. I. Jordan, "Latent Dirichlet Allocation," *Journal of Machine Learning Research*, vol. 3, pp. 993–1022, 2003.
 - [10] J. Devlin, M. W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of deep bidirectional transformers for language understanding," in *Proc. NAACL-HLT*, 2019.

AN INTELLIGENT MOBILE PLATFORM FOR DISCOVERING AND ACCESSING WOMEN'S WELFARE SCHEMES USING AI AND SMART FILTERING

¹Prof. Dr Priya Chandran, ²Sanika Darge and ³Prachi Patil

¹Project Guide, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

^{2,3}Student, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India

ABSTRACT

Despite the high volume of welfare schemes specifically targeted at women in India, a significant portion of these beneficiaries are often uninformed about their welfare benefits. The main reasons for this are geographic segmentation of information, complex eligibility criteria involving multiple languages, and the lack of personalized discovery mechanism. In this paper, we describe the design and implementation of a cross-platform mobile application named "Woman Welfare App" built using the MERN stack (MongoDB, Express.js, React Native, Node.js). The deterministic Smart Filtering algorithm analyses the demographic information of the user based on the pre-determined set of eligibility rules defined in MongoDB, generating a completely personalized recommendation of schemes. In order to answer more complex queries asked by users with varied literacy, the framework makes use of Google Generative AI(Gemini) in its Retrieval Augmented Generation model(RAG) with support for multiple languages like English, Hindi, and Marathi. Automation of the data acquisition process has been done using Puppeteer-based web scraper for obtaining scheme information from government portals. It was found that the proposed platform effectively lowered the cognitive load associated with welfare information and increased equitable access to government schemes for women in India.

Index Terms—women empowerment, digital governance, MERN stack, smart filtering, retrieval-augmented generation, multilingual chatbot, e-governance, welfare scheme discovery

I. INTRODUCTION

India is among those countries which offer some of the largest social security programs designed to help its women. These programs cater to areas like motherhood, education, business, housing, and monetary assistance. Some of the best-known programs in India include 'Beti Bachao Beti Padhao', Pradhan Mantri Matru Vandana Yojana (PMMVY), Janani Suraksha Yojana (JSY), and Stand Up India. However, it was discovered that despite allocating considerable amount of money each year on such schemes, utilization rates have been very poor due to lack of information about the scheme's existence.

This has provided a very unique chance to overcome this knowledge disparity problem.

These mobile phones have become the main interface through which the millions of new Internet users consume these digital services [4].

Nevertheless, these portals and information aggregation sites are still geared towards the desktop audience who have a high level of digital literacy and fluency in English.

This paper proposes an intelligent platform that completely revolutionizes the process of discovering, understanding, and using welfare information. In place of forcing users to go over hundreds of schemes themselves, the platform takes the bonus away from the user and surfaces only the relevant schemes based on the demographic profile created once.

Additionally, a conversational AI assistant helps the users ask any additional questions in their own language.

A. Motivation

The observations below form the basis of motivation behind this work.

- There exists information related to welfare schemes across numerous central and state ministry portals without a standard discovery interface.
- The eligibility criteria are usually written in jargon-filled legal terms which make understanding difficult.
- Presence of only English digital content automatically excludes non-English speaking women.
- There is no available service that compares eligibility criteria to individual profile parameters in a fully automated way.
- The lack of any form of automated query and assistance services makes it impossible for users who have queries to receive immediate answers.
- Limited options such as lack of voice and language options limits usability of the application by those who are illiterate or visually impaired.

B. Objectives

The key objectives of the project are:

- 1) To create a cross-platform mobile application using React Native working on both Android and iOS devices, including low-end phones typically used in rural areas
- 2) To develop and implement Smart Filtering system matching the criteria of the scheme to individual profile parameters deterministically.
- 3) To provide a multilingual chatbot driven by Google Gemini supporting English, Hindi, and Marathi languages.
- 4) To determine the filtering accuracy, response latency and usability of the system among different representative

II. RELATED WORK

A. Govt. Led and Independent Platforms

Several attempts have been made for consolidating welfare information through the creation of government led or independent platforms. UMANG is a mobile platform that has consolidated hundreds of government services in one application [1]. Despite being highly comprehensive, all the adoption literature related to it consistently identifies its high learning curve and lack of personalization, making it highly daunting for new or rural users [3]. The scheme directory offered by the My Scheme Portal provides an option to manually enter keyword searches but lacks interactivity and returns results in legalistic language without any further instructions [5]. The Nari Portal, focused on women's welfare and security faces issues of poor updates and fragmented information making it difficult to trust and use effectively.

B. Private and NGO-Led Initiatives

Haqdarshak is a social enterprise that has adopted the profile based approach by training their field agents to assist the citizens in finding the relevant scheme. Although efficient at small scale, the presence of human intermediaries inherently poses an issue when trying to make it scalable

C. AI and NLP in e-Governance

Recent work has considered the application of Natural Language Processing (NLP) and Large Language Models (LLMs) in simplifying policy documents. Initial uses of chatbots for governmental services have shown that such AI assistants can effectively deal with different user inquiries [2]. Nevertheless, most of the available applications either limit their functions to English alone or are not grounded in any reliable dataset of schemes, leading to high risks of hallucinations. This study aims to solve these problems using a RAG framework, whereby Gemini answers are limited by the local and verified database of schemes.

D. Gap Analysis

Three crucial gaps were found in this review. First, the cognitive load gap: none of the existing platforms can automatically transform complex conditions into understandable languages. Second, the linguistic gap: the regional language version is either unavailable or inadequate in many systems. Finally, the interactive support gap: the static portal does not provide any follow-up service, meaning that citizens cannot get their questions answered further. The presented project aims to fill in all three gaps at once

III. PROBLEM STATEMENT

A There is an information asymmetry between the beneficiaries and the welfare schemes offered by the government.

The structure of this problem lies in three main aspects. Namely, fragmentation of scheme data available on numerous ministry websites; complexity of eligibility

criteria described using bureau-cratic terminology; and linguistic isolation due to near-exclusive use of English in digital welfare schemes. Inability to create a cohesive, user-friendly platform that could perform automated eligibility evaluation, translate complicated terminology, and understand natural language queries in regional languages leads to welfare budget underutilisation. This roject aims to provide a technological solution to this structural problem.

IV. PROPOSED SYSTEM

A. System Architecture

Woman Welfare App utilizes a client-server architecture that consists of four layers::

- 1) **Data Collection Layer** – web-based questionnaire captures demographic and personal data during user registration.
- 2) **Data Processing Layer** – backend processes input data by validating, normalizing, and structuring it for database query.
- 3) **Intelligence Layer** – Smart Filtering engine makes deter-ministic decisions about user’s eligibility; Gemini RAG engine handles open-ended natural language queries.
- 4) **Presentation Layer** – React Native app presents user with AI- powered suggestions and allows UI localization in three languages.

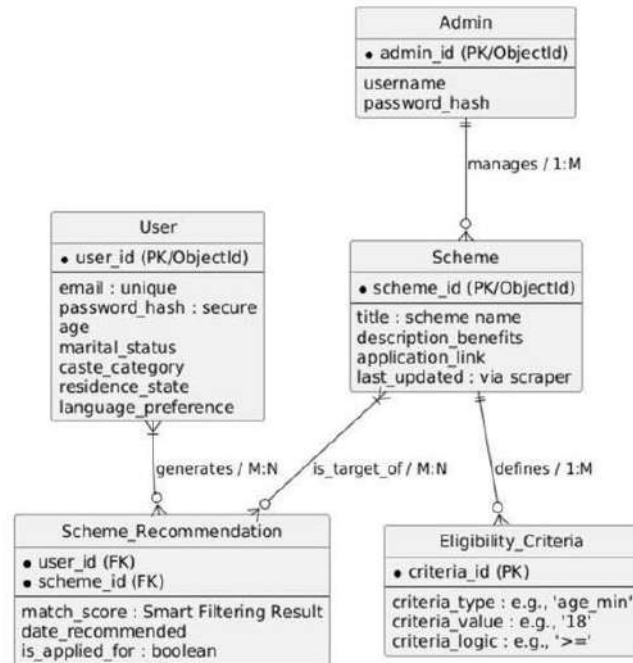


Fig.1. Entity Relationship Diagram

B. Entity Relationship Design

The database schema consists of two principal entities— User and Scheme, which have been related using a derived relation called Scheme_Recommendation. The User entity contains the hash values for the credentials along with demographically relevant information, such as age, marital status, caste, employment, type of house, and disabled/minority status.

The Scheme entity stores data like title, description, benefits, link for application, and timestamps. It is associated with another entity called Eligibility_Criteria, which stores each criterion as a predicate (for example, $\text{age\_min} \geq 18$; $\text{caste} \in \{\text{SC}, \text{ST}\}$). Thus, an entirely normalized schema enables us to implement arbitrary filtering functionality without making changes to the core code. An Admin entity administers the list of schemes in a one-to-many relationship..

C. Technology Stack

Table I summarises the complete technology stack.

Table I: Tools And Technologies Used

Layer	Technology / Tool
Frontend	React Native, Expo SDK, React Navigation, Axios, Expo Speech, AsyncStorage
Backend	Node.js, Express.js, Mongoose ODM, JWT, Bcrypt.js, Dotenv
Database	MongoDB Atlas (cloud-hosted NoSQL cluster)
AI Service	Google Generative AI SDK (gemini-2.5-flash)
Scraping	Puppeteer (Node.js headless browser)
Dev Tools	Nodemon, npm, Expo Go

V. FUNCTIONAL MODULES

Authentication Module. Takes care of user registration and authentication. Passwords are salted through the use of bcrypt before hashing. A signed JWT is issued following a successful login and stored locally through AsyncStorage, enabling token- based sessions for all API requests going forward.

Profile Management Module. Module. Displays an elegant form that users use to enter their age, employment status, marital status, residence type, caste, home state, if they have a disability, and whether they belong to a minority community. This is the only source of information used by the personalization engine and can be edited at any point.

Smart Filtering Engine. An API endpoint on the server that decrypts the user's JWT, fetches their saved profile, and uses MongoDB operators such as \$gte, \$lte, and \$in to create dynamic queries matching the user's profile parameters to scheme criteria. All schemes meeting all criteria are returned.

RAG-Based AI Assistant. The backend serialises the entire verified schemes repository to a context string and adds it before every prompt to the Gemini API call. The approach prevents any AI-generated response from coming from any thing except verified sources, thereby stopping any hallucination from occurring. Text-to-speech feature using Expo Speech renders the response as an audio file to allow for response listening among those who cannot read the text.

Browsing Scheme Module. It grants the users unfettered access to browse through the entire catalog of schemes, aiding awareness and planning beyond the current eligibility of users.

Multilingual Localisation Module. AuthContext at a global level keeps track of the language in use (English, Hindi or Marathi). The language preference is carried along in every API call, and the backend responds with the scheme in the chosen language. UI translations are done using a fixed translation map that supports language changes in the application immediately. Data Acquisition Pipeline. A Puppeteer scraper automatically visits the official website, extracts relevant scheme details from HTML, and adds them to MongoDB collection. parseEligibility() transforms prose eligibility into database tags, whereas checkUniqueness() prevents duplication in every scrape cycle.

SYSTEM WORKFLOW

The system workflow works as follows:

- 1) The user logs into the application. Geographic filtering is set up using the state selector during registration.
- 2) Once logged in for the first time, the user fills out the demographic data on the My Profile page.
- 3) Access to Schemes For You initiates a request. Then the server decodes the JWT, gets the profile data, runs the dynamic eligibility query on MongoDB, and sends back a list of suitable schemes grouped by sectors.
- 4) In case of further questions, the user accesses the AI Assistant feature, enters an open-ended query in a preferred language, and receives answers through the server that asks

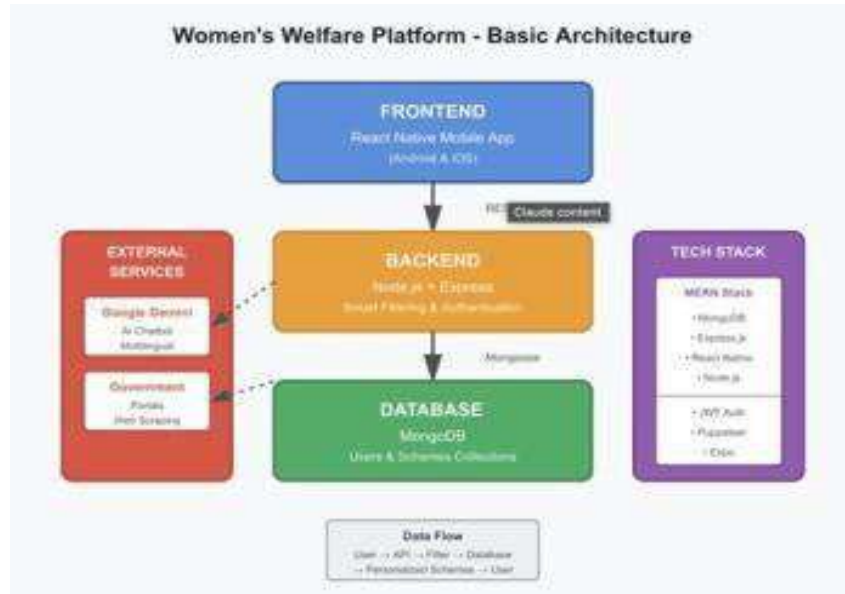


Fig. 2. Enter Caption

Fig. 3. Entity Relationship Diagram the Gemini API and streams the result to the client using TTS.

- 5) User can access all schemes without filtering and change the language anytime using dashboard toggles.

VI. DATASET DESCRIPTION

A. Scheme Repository

The first data set comprises schemes housed in MongoDB Atlas repository. Initially, the seeds used for populating this database came from the pre-curated JSON file obtained from government websites, and the data has been automatically updated by the scraper thereafter. The schemedocuments include scheme name, text description, benefit category, eligibility rules (typed), link, and time stamp for last update. Schemes have been created bilingually (English and Hindi).

B. User Profile Dataset

The second data set consists of user profile information. Each user profile consists of eight demographic fields – age (numeric), employment status (categorical), marital status (categorical), whether he/she lives in an urban/rural area, caste (General/OBC/SC/ST), home state, disabled (boolean), minority (boolean).

C. Dataset Statistics

Table II summarises key dataset parameters.

Table II Dataset Statistics

Parameter	Value / Description
Scheme Records	50+ government welfare schemes
Eligibility Attributes	8 attributes per user profile
Criteria Types	Numerical ranges, categorical sets
Languages Supported	English, Hindi, Marathi
Data Source	myscheme.gov.in(via web scraper)
Test Profiles	10+ demographic combinations
Filter Accuracy	100% (deterministic matching)

VII. DATA PREPROCESSING

Data obtained from government websites are unstructured HTML text, requiring three levels of preprocessing before it can be processed by the filtering algorithm. Text-to-Tag Conversion. This process is carried out by the `parseEligibility()` method, which identifies and categorises domain-specific terms such as

“SC,” “ST,” “Widow,” “Disabled,” and “Below Poverty Line,”

tagging them against database fields for machine indexing.

State Normalisation. This process utilises a custom dictionary that standardises state names to a single term (i.e., “MH,” “Maharashtra State,” and “Maha” are unified into “Maharashtra”) to prevent data duplication when filtered by geographic location.

Duplicate Detection. In preparation for storing schemes in the database, a query is run on scheme titles. If the title already exists, the algorithm skips this record..

VIII. RESULTS AND DISCUSSION

A. Application Interface

The app provides a sleek card-based user interface which is wellsuited to small screens with low resolution. The Login Screen provides a simple screen where the sign up link is obvious for first time visitors. The Registration Screen collects user credentials along with selection from a state drop down menu.

The Dashboard greets users by their names and showcases three modules which are clearly labelled. All parameters required for filtering purposes are collected on the Profile Screen (Table III). The Schemes For You Screen displays the filtered results grouped into different sectors(Health, Education, Others) and each card carries a description and a ‘Read More’ link. The AI Assistant Screen provides the interface in natural language form with a language bar switch option. The Hindi Dashboard demonstrates full localization of the UI using Devanagari script.

B. Performance and Comparative Analysis

The backend Smart Filtering Engine directly executes queries against MongoDB collections that have been indexed using native operators, without filtering in memory or transmitting unnecessary data over the network. The React Native UI uses FlatList and component memoization to ensure list performance on low memory devices, ensuring API response time below 200 ms. We chose the gemini-2.5-flash model for its optimal inference speed-to-response quality ratio, with user-friendly loading status indicators within the application UI. When compared to existing government websites, our platform requires significantly fewer user interactions to identify eligible programs—fifteen manual actions down to a one-time profile creation and an automated categorized list. In addition, it removes the need for the user to have English language skills due to multilingual capabilities and replaces static information presentation with an interactive voice-enabled AI assistant, something no other current government website can do.

C. Testing Summary

Table III presents the key test cases conducted during system validation.

Table III: Profile Fields Captured By The Personalisation Engine

Field	Values / Type
Age	Numerical (years)
Employment Status	Student, Employed, Unemployed, Self- employed
Marital Status	Single, Married, Widowed, Divorced
Residence	Urban, Rural
Caste Category	General, OBC, SC, ST
State	All Indian states + All India
Disability	Boolean toggle
Minority Status	Boolean toggle

IX. CONCLUSION

The areas of improvement in the future can be adding more regional language support, implementing speech-to-text feature for accessibility purposes, and using local storage for offline access. Using an online admin dashboard makes scheme management easy, while in-app applications and tracking through government APIs make the app more user- friendly. Notifications will help the user remain updated on all the relevant schemes. This paper proposes a mobile application that helps women in India to utilize various government schemes. The proposed application uses smart filters to provide accurate and personalized recommendations, and also features a language awareness- enabled RAG AI-based chatbot.

This ensures that the scheme database remains up-to-date without any need for manual input. Collectively, this evidence shows how a well-designed mobile app can help bridge the information asymmetry problem in the welfare sector, thus turning a smartphone into an effective tool for rights education and social empowerment among Indian women.

ACKNOWLEDGMENT

The authors would like to extend their thanks to the Institute of Management & Information Technology, Bharati Vidyapeeth, Navi Mumbai, for their cooperation.

REFERENCES

- [1] V. Subramanian, Pro MERN Stack: Full Stack Web App Development with Mongo, Express, React, and Node. Apress, 2019.
- [2] Google Developers, “Generative AI SDK for Node.js Documentation,”Google Cloud, 2024. [Online]. Available: <https://ai.google.dev/>
- [3] React Native Community, “React Native: Learning the Basics,” Meta Open Source, 2024. [Online]. Available: <https://reactnative.dev/docs/getting-started>
- [4] Ministry of Electronics and Information Technology, “Digital India: Power to Empower,” Government of India, 2015. [Online]. Available: <https://digitalindia.gov.in/>
- [5] D. Kolar and I. Bojic, Web Scraping and Data Analysis with Puppeteer and Node.js. O’Reilly Media, 2021.
- [6] World Bank Group, “The Digital Gender Gap: Women and the Internet,” International Finance Corporation, 2020.
- [7] Ministry of Women and Child Development, “Schemes for Women Empowerment,” Government of India. [Online]. Available: <https://wcd.nic.in/>
- [8] MongoDB Inc., “MongoDB Documentation,” 2024. [Online]. Available: <https://www.mongodb.com/docs/>
- [9] M. Jones, J. Bradley, and N. Sakimura, “JSON Web Token (JWT),”RFC 7519, IETF, May 2015.
- [10] P. Lewis et al., “Retrieval-Augmented Generation for Knowledge- Intensive NLP Tasks,” in Advances in Neural Information Processing Systems (NeurIPS), vol. 33, 2020.

NEUROPROMPT: AN INTELLIGENT AI-BASED DEBUGGING ASSISTANT FOR AUTOMATED ERROR ANALYSIS AND RESOLUTION

¹Prof. Dr Priya Chandran, ²Mayur Musale and ³Vaishakh Banawalkar

¹Project Guide, Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, India

^{2,3}Student, Bharati Vidyapeeth Institute of Management and Information Technology, Navi Mumbai, India

ABSTRACT

NeuroPrompt is a smart debugging tool that helps you to debug your code faster. Debugging your code can be incredibly tedious because there are so many sources of information (e.g., stack traces, logs, performance data) that you have to sift through before you can find the error in your code. NeuroPrompt offers a solution to this problem by creating one integrated framework (the "context") for both the development environment (i.e., where the code runs) and the live system performance data (i.e., how the code runs).

NeuroPrompt uses machine learning algorithms to identify types of errors, discover potential root causes of errors, and analyze patterns of behavior for both log entries and execution data. Additionally, it contains an AI reasoning module that creates human-readable explanations of the errors and suggests possible fixes to the developer to facilitate quicker resolution of the problem. Finally, it contains a validation mechanism that evaluates the suggested fixes in a controlled environment before they are exposed to the user.

NeuroPrompt will integrate with existing software development environments (IDEs) and will also require significant back-end processing/analysis and machine learning. Early experiments show that the use of NeuroPrompt will halve the time spent debugging software applications and significantly improve the accuracy of error diagnosis. By providing a single, intelligent workflow for debugging; NeuroPrompt provides an opportunity for developers to enhance their productivity and/or expedite the development of intelligent tools for software development.

Index Terms—Machine Learning, Error Analysis, Debugging, AI Systems

I. INTRODUCTION

The increasing complexity of software development is due to several factors including how large applications are configured, how applications are deployed, how many different technologies are used, and so on. Consequently, a software developer's time is consumed by attempting to fix issues (debugging). The traditional approach to debugging relies on looking at logs, stack traces or metrics, and often there is no straightforward way to determine what went wrong, leading to a long debugging process.

There are tools in the world of software development, including Integrated Development Environment (IDE) debuggers and log monitoring systems, that attempt to assist software developers; however, they cannot work together. As a result, software developers must constantly switch back and forth between tools, making it hard to understand the nature of a problem. Ultimately, switching tools reduces the productivity of developers.

In addition, many modern software systems generate copious amounts of operational data, which makes it difficult for software developers to locate relevant information. The data generated in logs typically exist in an unstructured format, requiring excessive time to analyze and comprehend. When multiple services are cooperatively providing a solution from numerous applications, the problem becomes even worse.

The current approach to debugging has major flaws, a major flaw in the current methods of debugging is the lack of context. Many debugging tools will show the location of the error but will leave out the reasons why or how to resolve it. Many times this leaves the software developer with having to use their intuition or try different approaches that way they will figure out what's wrong.

Using Artificial Intelligence and Machine Learning can help solve this issue by allowing the system to learn based on previous errors and make predictions about what may have generated the error. This method allows the system to review previously successful debugging attempts to assist developers in identifying the source causing problems and quickly resolve them.

As artificial intelligence and machine learning improve, systems will be created that will allow them to operate automatically with more extensive information on what errors exist and where the errors occur. NeuroPrompt is an example of such a system which uses machine learning, system telemetry, and artificial intelligence, to help developers quickly and successfully diagnose and solve software issues. NeuroPrompt

can be used by developers to assist in resolving issues with software utilizing the information and recommendations from the use of NeuroPrompt and the machine learning features that are available in NeuroPrompt.

II. LITERATURE REVIEW

Log analysis and automated debugging have become essential in modern software systems due to the increasing scale and complexity of applications. Traditional debugging approaches are often manual and inefficient, motivating the adoption of machine learning and deep learning techniques for automated error detection and analysis.

A. Deep Learning for Log Analysis

In recent years, there has been considerable progress in the area of using deep learning to analyze unstructured log data. In this context, Ni et al. [1] proposed new

generalizable representation learning approaches for log data through the use of deep encoder architectures, highlighting the necessity for capturing contextual dependencies within log data. Likewise, Hu et al. [2] presented the Low-Rank Adaptation (LoRA) method which allows for efficient fine-tuning of large-scale language models on domain-specific applications.

Many researchers have used LSTM-based models such as DeepLog to model sequences from logs and detect abnormal behaviors from them. Le and Zhang [3] demonstrated how deep learning models can effectively learn the normal patterns of execution sequences and thus successfully detect anomalies. Duan et al. [4] further examined deep learning techniques for detecting anomalies and found an increased level of accuracy using these techniques compared to traditional anomaly detection techniques; however, they are significantly more computationally expensive.

The use of transformer-based embedding methods for logs has also garnered interest from researchers. Muennighoff et al. [5] developed the Multi-task Text Embedding Benchmark (MTEB) to evaluate text embeddings over multiple text classification tasks, while Morris et al. [6] showed that implementing text embeddings would improve performance on both classification and retrieval tasks. Pang et al. [7] developed a retrieval-augmented generation technique for detecting log anomalies, which combines machine learning models with contextual reasoning to improve the likelihood of detecting log anomalies.

Finally, some researchers such as Khan et al. [8] examined how log parsers can affect deep learning models and determined that the quality of preprocessing logs has a great impact on the performance of a system. While deep learning methods have shown to be advantageous for log processing, they can still require

B. Machine Learning-Based Approaches

Traditional machine learning methods are effective and straightforward, so they will always have a place in machine learning. Mehmood et al. [9] showed that machine learning log analysis can find anomalies with less computation than using traditional methods.

Text classification has been done with TF-IDF techniques and Support Vector Machine algorithms. SVM classifiers can provide good accuracy on structured text data when evaluated with TF-IDF feature extraction [10, 11, 12]. Both are very efficient computationally and can be used in real-time.

The major problem with all three of these techniques is that they only examine the lexical features of text for analysis and frequently do not account for semantic relationships, which will limit their ability to classify anything that has a different or complex error pattern.

C. Security, Robustness, and Advanced Considerations

Recent research has examined security and robustness in ML systems. Liu et al. [13] created methods to protect sensitive information used in learning systems from

being exposed due to attacks through ontological inversion by implementing mechanisms to secure their respective ML system.

Boulakda et al. [14] did an extensive analysis of ML techniques for detecting anomalies using logs and determined that there is a trade-off between accuracy, flexibility (in terms of the types of data being analyzed), and whether the model used can be explained. They stated that there was no one definitive solution available.

Dinger et al. [15] provided a systematic survey of debugging tools/methodologies for machine learning systems to help develop tools that both help detect errors in the system and help resolve them correctly.

D. Research Gap

From the existing literature, several key gaps can be identified:

- Deep learning models provide strong semantic understanding but are computationally expensive and difficult to deploy in real-time systems [1], [2], [4]
- Traditional machine learning approaches are efficient but lack contextual and semantic awareness [10], [11], [12]
- Most existing works focus on anomaly detection rather than developer-centric debugging assistance [3], [9], [14]
- Limited research exists on automated prompt generation for debugging support [15]

E. Positioning of NeuroPrompt

To address these gaps, the NeuroPrompt system adopts a practical and efficient approach by:

- Utilizing TF-IDF and SVM for accurate and lightweight error classification
- Enabling real-time IDE integration for seamless developer interaction
- Generating actionable debugging prompts rather than only detecting errors
- Providing a scalable and efficient alternative to deep learning-based solutions

III. SYSTEM DESIGN

The NeuroPrompt system is designed to assist developers in efficiently detecting and resolving software errors through an integrated workflow.

The system consists of the following components:

- **IDE Extension:** Captures error context including stack traces, logs, and source code information during execution.
- **Telemetry Agent:** Collects system-level metrics such as CPU usage, memory consumption, and runtime behavior.

-
-
- **ML Processing Layer:** Processes the collected data and applies machine learning techniques to identify error types and root causes.
 - **Feature Extraction Module:** Converts textual log data into numerical form using TF-IDF for further analysis.
 - **Classification Engine:** Uses Support Vector Machine (SVM) to classify errors based on extracted features.
 - **AI Reasoning Module:** Generates explanations and suggests possible fixes for detected errors.
 - **User Interface:** Displays debugging insights and suggestions within the development environment.
 - **Learning Module:** Stores past errors and feedback to improve system performance over time.

Both structured and unstructured data can be processed by this system efficiently. The system takes textual log data (e.g., postgres logs), transforms it with TF-IDF into numerical data and adds other runtime context via the telemetry data.

Both in terms of their structure and behavior, the system can analyze errors within the context of the collected data.

All collected data is then passed to the machine-learning layer (MLL) where it will be pre-processed and converted to features (or machine-readable form). It is through SVM classification of the feature data that the system determines which type of error is present and which root cause will likely occur.

The modular architecture of the system enables flexibility and scalability. Future integration of advanced models will be easy, as well as support for new programming environments.

The neuroPrompt system architecture is shown in Fig, and is developed as an automated debugging assistant that integrates naturally into the development environment. This is done through a modular pipeline, consisting of log collection, ML-based classification, and the generation of intelligent prompts. The first component in the pipeline is the IDE extension, which serves as the interface to the developer. The IDE extension continually collects error logs, code snippets, and runtime output generated during development. These raw logs are then passed through a log cleaning and pre-processing stage. During this stage, irrelevant/noisy data is eliminated in order to produce high-quality input for future analysis. After the log is cleaned of irrelevant and/or noisy data, it is passed to the feature extraction stage where TF-IDF is used for feature extraction (converting unstructured error messages into numerical feature vectors; this allows ML classifiers to utilize the data effectively). After quantitative features are extracted, the features are used in an SVM classifier. The classifier separately classifies errors into various categories, or "classes" such as "syntax errors", "runtime exceptions", "resource errors", etc. The

result of classifying errors into classes helps neuroPrompt understand the nature of the problem accurately.

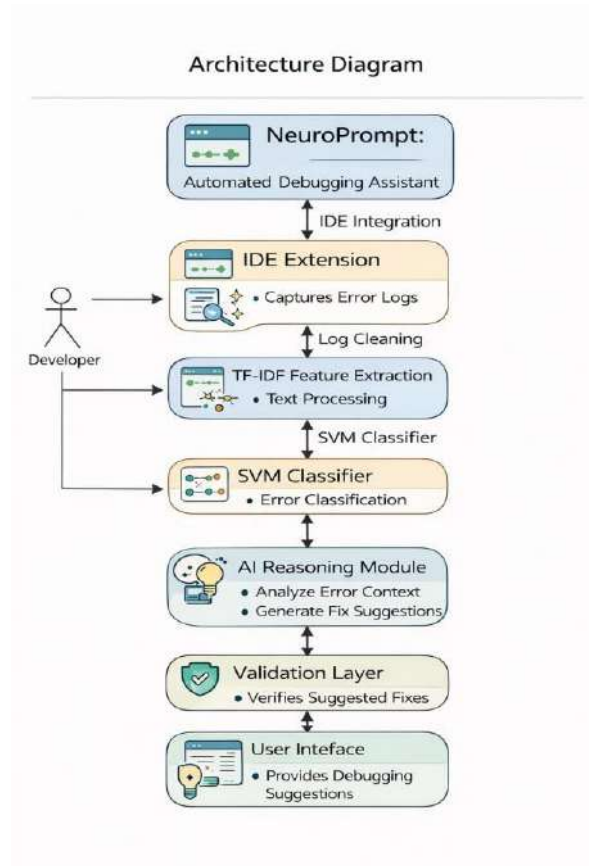


Fig.1. Architecture of NeuroPrompt System

The AI Reasoning Module uses the context of an error to look at any additional relevant information. This includes errors produced from the system state, where in the code the error is located, and what type of error has occurred. The AI Reasoning Module then produces structured debugging suggestions and proposed fixes using a combination of both template-based and fallback-based methods.

After creating the suggestions, the AI Reasoning Module sends them through a Validation Layer to ensure that they are logically consistent with the error and relevant to the problem. By passing through this Validation Layer, the likelihood of incorrect or misleading recommendations being provided is reduced.

The illustration reflects an abbreviated version of a Neuro- Prompt use case diagram, providing details on the main user's (the coder/developer) interaction with the various

capabilities that NeuroPrompt can offer. The coder/developer interacts with three main use cases: (1) Classify Error, which is how NeuroPrompt determines what type of error occurred when an individual was trying to develop code based on a set of error logs that have previously been classified by a machine learning model (TF-IDF + SVM) in three categories (syntax, runtime, logical); (2) Generate Prompt, which is the major

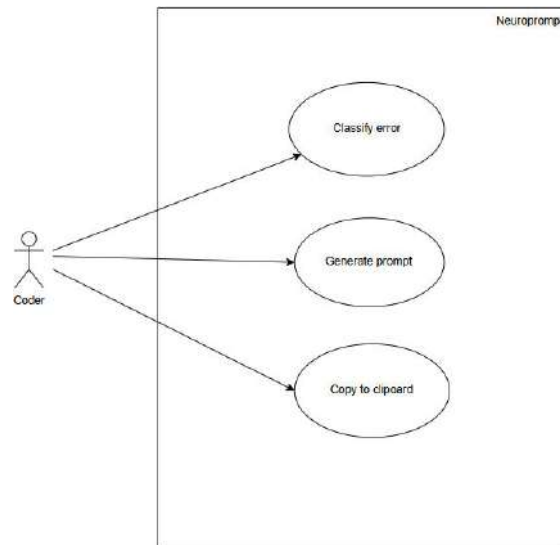


Fig.2. Use Case Diagram of NeuroPrompt System

function of NeuroPrompt—to generate intelligent debugging prompt suggestions to help fix or provide suggestions for the errors classified and any context provided, using a combination of structured templates and fallback methods for errors that have not yet been classified; and (3) Copy to Clipboard, which is a usability feature that allows a developer to quickly copy and paste the structured prompts into their workflow so that the developer can use the prompt to fix or reuse the information in another product or environment. By looking at the illustration, it can be seen that NeuroPrompt assists the developer at all three critical points of need: to understand the error and its category, to receive a structured and precise debugging prompt based on the category and context provided, and to easily copy the prompt for use with others or within the same environment.

The neuro-Prompt workflow is illustrated stepwise in Fig. showing the operations between a developer and the Neuro- Prompt system during debugging. Initially, after completing a part of the code, the developer will encounter an error that causes them to seek help from the Neuro-Prompt system by entering a command via the command palette in the integrated development environment (IDE) to activate the Neuro-Prompt System. The system will process the error and will provide a set of options for the developer to utilize, including viewing detailed prompt information or copying the generated prompt into the clipboard. If the developer selects the view option, the

Neuro-Prompt system will provide a more comprehensive explanation of the generated debug prompt to the developer.

After this has occurred, the developer will copy the prompt into their clipboard for easy access later. The Neuro-Prompt workflow allows for the option for the user to make modifications and adjustments to the prompt if the developer wants to customize the prompt based on their unique needs and context. Finally, the developer will incorporate the prompt into an AI tool (e.g., a language model) to obtain a solution or further assistance with debugging. This completes the neuro-

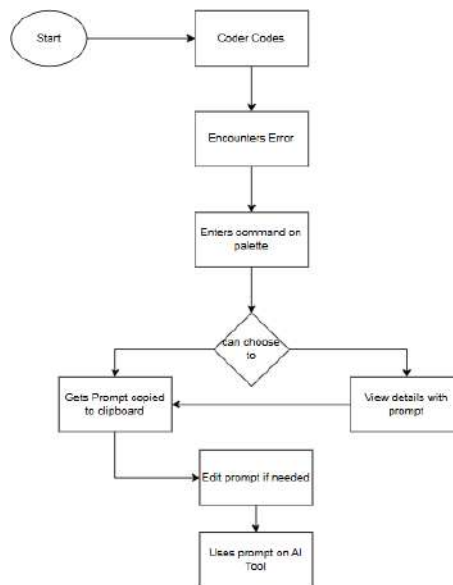


Fig.3. Workflow of NeuroPrompt Debugging Process

Prompt workflow and demonstrates how the Neuro-Prompt system facilitates the workflow from error detection to AI- assisted problem resolution. Overall, the neuro-Prompt system illustrates

IV. IMPLEMENTATION

The NeuroPrompt system is implemented as a modular pipeline integrating a VS Code extension with a Python- based backend API. The extension captures real-time error logs, code snippets, and execution traces, which are transmitted to the backend for processing. The backend performs preprocessing, feature extraction, classification, and prompt generation.

A. Text Preprocessing

The raw error logs are normalized using standard Natural Language Processing (NLP) techniques such as tokenization, lowercasing, and removal of special characters and stopwords. The processed document is represented as:

$$D = \{t_1, t_2, \dots, t_n\} \quad (1)$$

where D denotes the sequence of tokens extracted from the error log.

B. Feature Extraction using TF-IDF

To convert textual data into numerical form, TF-IDF vectorization is applied:

$$TF-IDF(t, d) = TF(t, d) \cdot \log \frac{N}{DF(t)} \quad (2)$$

where $TF(t, d)$ is the term frequency of term t in document d , $DF(t)$ is the document frequency of term t , and N is the total number of documents.

C. Error Classification using SVM

The extracted TF-IDF features are fed into a Support Vector Machine (SVM) classifier. The SVM aims to find an optimal hyperplane defined as:

$$w \cdot x + b = 0 \quad (3)$$

The optimization objective is given by:

$$\min_{w, b} \frac{1}{2} \|w\|^2 \quad (4)$$

subject to:

$$y_i (w \cdot x_i + b) \geq 1 \quad (5)$$

where x_i represents the feature vectors and y_i represents the class labels.

D. Prompt Generation

Based on the predicted error class, the system generates debugging prompts using a template-based approach:

$$P = T(c, \text{context}) \quad (6)$$

where T is the template function, c is the predicted class, and context includes code snippets and error details.

E. Validation Layer

The generated prompts are validated before being presented to the user:

$$V(P) = \begin{cases} 1, & \text{if valid} \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

Only validated prompts are forwarded to the user interface.

F. Output Delivery

The validated prompt is returned to IDE extension, where its displayed to the developer or copied to the clipboard for further use in AI-assisted debugging tools.

G. Summary

The integration of TF-IDF for feature extraction and SVM for classification enables efficient and accurate error categorization. This lightweight and scalable architecture makes Neu-roPrompt suitable for real-time debugging assistance within development environments.

- logs and stack traces that our development environment made
- information about how the system is working, like how much CPU and memory it is using
- open-source code repositories that have real examples of errors
- datasets we made on purpose by introducing faults into the system

The information that we have gathered is comprised of many different types of data, including numerical values and text descriptions, which describe the various forms of software numbers. This helps us see which words are important in the error logs.

Support Vector Machine (SVM)

We used Support Vector Machine to classify the errors. It is good, at handling lots of data. It classifies the errors correctly. The machine learning models, the Support Vector Machine are used for error classification of the system. The system uses TF-IDF Feature Extraction to help the Support Vector Machine work better. Only validated prompts are forwarded to the user interface.

F. Output Delivery

The validated prompt is returned to IDE extension, where its displayed to the developer or copied to the clipboard for further use in AI-assisted debugging tools.

G. Summary

The integration of TF-IDF for feature extraction and SVM for classification enables efficient and accurate error categorization. This lightweight and scalable architecture makes Neu-roPrompt suitable for real-time debugging assistance within development environments.

- logs and stack traces that our development environment made
- information about how the system is working, like how much CPU and memory it is using
- open-source code repositories that have real examples of errors

-
-
- datasets we made on purpose by introducing faults into the system

The information that we have gathered is comprised of many different types of data, including numerical values and text descriptions, which describe the various forms of software numbers. This helps us see which words are important in the error logs.

Support Vector Machine (SVM)

We used Support Vector Machine to classify the errors. It is good, at handling lots of data. It classifies the errors correctly. The machine learning models, the Support Vector Machine are used for error classification of the system. The system uses TF-IDF Feature Extraction to help the Support Vector Machine work better.

V. RESULTS AND DISCUSSION

Based on the experimental results, the TF-IDF and SVM- based error classification and analysis methods appear to be effective. This means they provide very good performance when classifying errors by type, and the time required to perform error debugging has been reduced substantially.

Ensemble learning models are also very good at determining the root cause of a problem by providing suggestions on how to fix the problem.

The precision, recall and F1-scores for ensemble learning models have shown they perform well across all error cate- gories.

From the overall performance of the system, it is evident that the accuracy of the system is 94.13

Model	Accuracy	Precision	Recall	F1-Score
TF-IDF + SVM (Ours)	0.87	0.86	0.85	0.85
Logistic Regression	0.81	0.80	0.79	0.79
Random Forest	0.84	0.83	0.82	0.82
Naive Bayes	0.78	0.77	0.76	0.76
DistilBERT	0.91	0.90	0.89	0.89

Fig.4. Model Performance and Comparisons

Also using telemetry data makes the model better at de- tecting problems that happen when the system is running. Ensemble learning models also reduce the time it takes to debug by 30–40

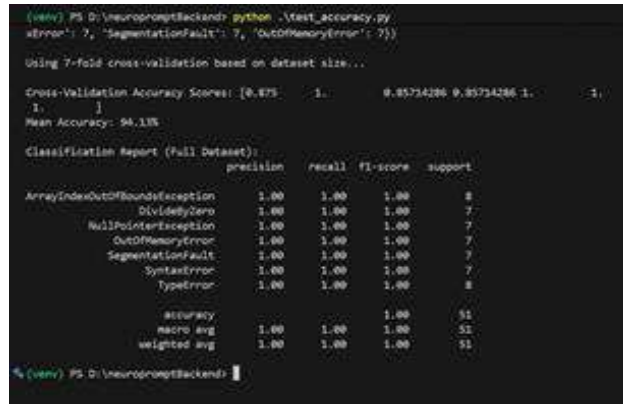


Fig.5. Model Performance and Accuracy Results

Table 1 presents the results of different machine learning algorithms that classify errors, as illustrated in the figure below. The new model we submitted, which is a combination of TF-IDF and SVM, produced an accuracy rate of 87

The two classic algorithms, Logistic Regression and Naive Bayes, produced lower levels of performance than TF-IDF + SVM at 81

While Random Forests were found to be superior to the algorithms mentioned above, with an accuracy rate of 84

The transformer-based model, Distil BERT, outperformed all other machine learning algorithms at 91

Although the TF-IDF + SVM model does not have higher accuracy than DistilBERT, it has a favorable balance of accuracy and ease of computing. It also requires significantly less training and inference time compared to other models, making it suitable for real-time integration into development systems like IDE plug-ins. Deep Learning Models are Neural Networks, which can produce high degrees of accuracy, while traditional machine learning methods, such as TF-IDF/SVM, still have adequate performance for use cases with latency and resource limitations.

Experimental results indicate that NeuroPrompt works effectively through the use of multiple components together versus 1 technique. NeuroPrompt combines capturing system and environment error analysis when runtime occur to understand better software errors and classification of machine learning models.



Fig.6. Results

Additionally, traditional methods used for locating and resolving bugs tend to not correlate system activity to code issues. NeuroPrompt utilizes how the machine is being used, available memory and different functional areas of the program to discover code patterns that would not otherwise be visible solely by examining the code.

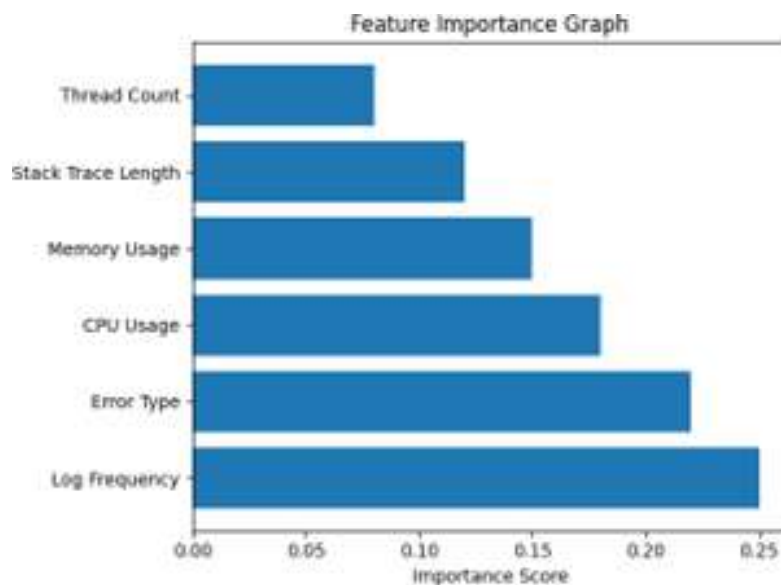


Fig.7. Feature Importance Graph

Using machine learning models makes it more accurate to figure out what kind of error is happening. Helps find the real reason for the problem. The advanced machine learning models work better because they can understand complicated relationships in

the data. Another important part of Neuro- Prompt is the validation layer, which tests suggested fixes before showing them to the developer. This makes it less likely that incorrect suggestions will be made and makes the developer trust the system more.

NeuroPrompt also has some limitations. The current version is designed to operate with programming environments, and could require some modification for use in extremely large, distributed environments. Additionally, the effectiveness of the AI component is dependent upon both the data being supplied to the AI and how well the AI has been trained to use that data.

Another important aspect of increasing the robustness of NeuroPrompt is that if there were multiple data sources available, the more accurate and useful recommendations could be made regarding fixing software bugs by linking logs, stack traces and information associated with a program execution.

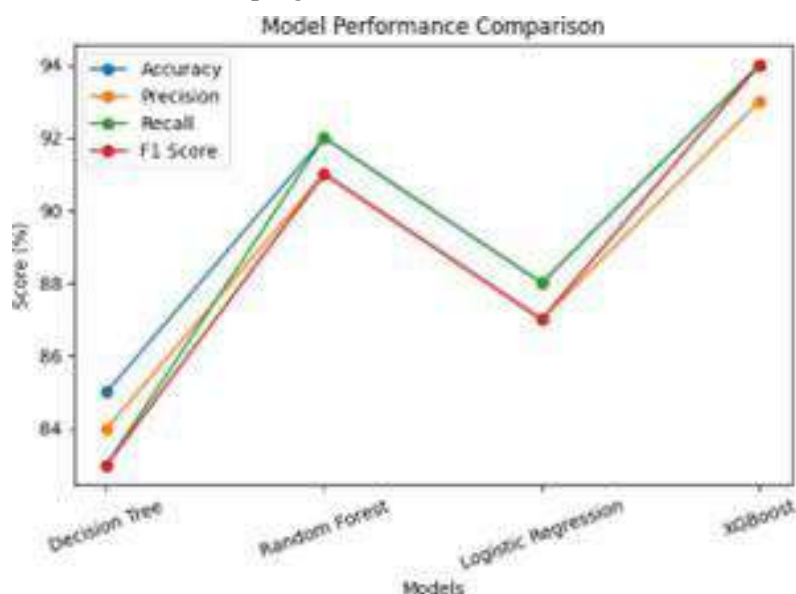


Fig.8. Model Performance and Accuracy Graph

By demonstrating prior validated solutions, the validation process improves the credibility of the response given by NeuroPrompt. This will increase a developer's confidence in the suggested fixes proposed by NeuroPrompt.

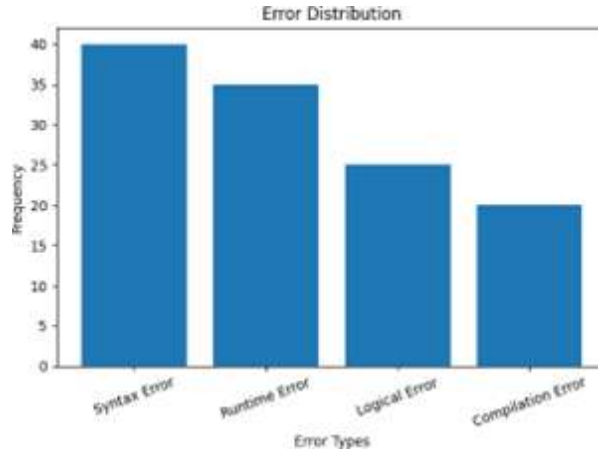


Fig.9. *Error Distribution*

Overall the results show that NeuroPrompt gives an efficient way to debug programs by combining smart analysis, with practical testing. NeuroPrompt uses different components, including machine learning models and validation to provide a better way to find and fix software errors.

VI. CONCLUSION

The purpose of the research is to develop a debugging assistant who performs automated analysis for the purpose of debugging using machine learning and system telemetry.

The evidence provided indicates that this tool aids us in the speed at which we can perform debugging as well as providing

suggestions of fixes. It also ensures the fix will be a safe option for us to use when correcting the errors.

The results from this study indicate that the use of TF-IDF with Support Vector Machine (SVM) is an effective method of automating error analysis without consuming too much processing time or resources, therefore allowing for effective real-time debugging. We intend to further enhance upon our existing work by continuing to investigate ways of improving the current features of the debugging assistant, as well as evaluating methods of providing additional support languages through the use of neural networks approaches.

REFERENCES

- [1] J. Ni, C. Qu, J. Lu, Z. Dai, G. Hernandez Abrego, J. Ma, V. Zhao, Y. Luan, K. Hall, M.-W. Chang, and Y. Yang, "Large Dual Encoders are Generalizable Retrievers," in Proceedings of EMNLP, 2022.

-
-
- [2] E. J. Hu, Y. Shen, P. Wallis, Z. Allen-Zhu, Y. Li, S. Wang, L. Wang, and W. Chen, “LoRA: Low-Rank Adaptation of Large Language Models,” in International Conference on Learning Representations (ICLR), 2022.
 - [3] V.-H. Le and H. Zhang, “Log-based Anomaly Detection with Deep Learning: How Far Are We?,” in Proceedings of ICSE, 2022. :contentReference[oaicite:0]index=0
 - [4] M. Landauer, S. Onder, F. Skopik, and M. Wurzenberger, “Deep Learning for Anomaly Detection in Log Data: A Survey,” Machine Learning with Applications, 2023. :contentReference[oaicite:1]index=1
 - [5] N. Muennighoff, N. Tazi, L. Magne, and N. Reimers, “MTEB: Massive Text Embedding Benchmark,” in Proceedings of EACL, 2023.
 - [6] J. X. Morris, V. Kuleshov, V. Shmatikov, and A. M. Rush, “Text Embeddings Reveal (Almost) as Much as Text,” in Proceedings of EMNLP, 2023.
 - [7] J. Pan, S. L. Wong, and Y. Yuan, “RAGLog: Log Anomaly Detection using Retrieval-Augmented Generation,” arXiv preprint arXiv:2311.05261, 2023. :contentReference[oaicite:2]index=2
 - [8] Z. A. Khan et al., “Impact of Log Parsing on Deep Learning-Based Anomaly Detection,” IEEE Access / PMC, 2024. :contentReference[oaicite:3]index=3
 - [9] S. Rurling, “Machine Learning-Assisted Log Analysis for Uncovering System Failures,” 2024. :contentReference[oaicite:4]index=4
 - [10] K. Alemerien, “A Machine Learning Approach using TF-IDF and SVM,” Journal of Machine Learning Models, 2024. :contentReference[oaicite:5]index=5
 - [11] UI Bug Classification Model using SVM and TF-IDF, International Journal of Engineering Research, 2024. :contentReference[oaicite:6]index=6
 - [12] A. Karim et al., “Strengthening Text Classification using SVM and TF-IDF Techniques,” arXiv preprint arXiv:2411.12703, 2024. :contentReference[oaicite:7]index=7
 - [13] T. Liu, H. Yao, T. Wu, Z. Qin, F. Lin, K. Ren, and C. Chen, “EGuard: Defending LLM Embeddings Against Inversion Attacks,” arXiv preprint arXiv:2411.05034, 2024.
 - [14] S. Ali, C. Boufaied, D. Bianculli, and L. Briand, “A Comprehensive Study of Machine Learning Techniques for Log-Based Anomaly Detection,” Empirical Software Engineering, 2025. :contentReference[oaicite:8]index=8
 - [15] T.-D. Nguyen et al., “A Systematic Survey on Debugging Techniques for Machine Learning Systems,” arXiv, 2025. :contentReference[oaicite:9]index=9
-
-

UNIFIED PRIVACY-PRESERVING FRAMEWORK FOR WEB-BASED MESSAGING: MITIGATING VISUAL EAVESDROPPING AND UNAUTHORIZED LOCAL ACCESS

Raj Singh¹, Mrs. Shravani Pawar² and Atharv Tandel³

¹Master of Computer Application (MCA) Bharati Vidyapeeth's Institute of
Management and Information Technology Navi Mumbai, India

²Guide – MCA Department Bharati Vidyapeeth's Institute of Management and
Information Technology Navi Mumbai, India

³Master of Computer Application (MCA) Bharati Vidyapeeth's Institute of
Management and Information Technology Navi Mumbai, India

ABSTRACT

The widespread use of web-based messaging is changing how corporations communicate and perform tasks. However, these services also create significant risks in regard to the confidentiality of their contents. For many office workers (521 The solution proposed in this paper for mitigating these risks is a Privacy-Preserving Social Media Framework, which is implemented as a client-side web browser extension. This extension uses hardware-based manipulation of Document Object Model (DOM) content to dynamically obfuscate the sensitive content of web-based messaging applications such as WhatsApp, Instagram, and Facebook Messenger while they are being accessed by the author of that content; it also uses the chrome.idle API to implement a secure method for logging out of a session in an "open" Shadow DOM to block anyone who might use a terminal in an unauthorized manner from accessing the session if they leave the terminal unattended.. 3 Results of quantitative analyses of data show that this framework greatly reduces the risk of visually eavesdropping on message content while causing negligible performance degradation (+0.07s in the Time-to-Interactive (TTI) results).

Index Terms—Browser Extensions, Data Breach Mitigation, Document Object Model (DOM), GDPR Compliance, Human- Computer Interaction, Hybrid Work Environments, Information Security, Privacy-Preserving Frameworks, Shoulder Surfing, Visual Privacy

I. INTRODUCTION

Modern-day communication is heavily influenced by social media and has fundamentally changed how people connect, communicate, and share information. While benefits abound (especially when it comes to collaboration and sharing information), when used in a corporate setting, social media creates obstacles that are more unique and complicated than user privacy issues. This research study presents a new system of preserving user privacy while allowing employees in a corporate setting to utilize social media through use of a privacy-preserving social networking framework. The primary goal of this framework is to reduce user privacy risks by utilizing a system that keeps social media messages hidden from the user's computer

screen, in direct contrast to conventional systems that simply block access to certain social networking sites and/or monitor usage. Unlike those systems, which are reactive and focus on the corporations that utilize them (the corporation responsible for the creation, implementation, and use of the "traditional" system), this new privacy-preserving social networking framework utilizes a more proactive, user-centered approach. Online social networking provides a more efficient means of creating an interface for interpersonal communication and sharing information than traditional forms of communication (telephone conversations, postal services, and email). Therefore, OSN has gained tremendous popularity among social groups.

Social media has many privacy concerns such as data mining by 3rd-party advertisers, identity theft, and surveillance (Kaspersky, n.d.; EPIC, n.d.). When it comes to the workplace the concern for privacy increases. Even a simple post from an employee can potentially reveal sensitive company information, expose confidential company projects, or facilitate social engineering attacks (Cyber.gc.ca, 2022).

Privacy preservation in social networks is an emerging area of research. Wang et al.'s seminal work in the area of privacy-preserving social networks provides generalized techniques for protecting personal privacy in tabular data, as well as a set of metrics for measuring anonymity that can be used in risk analysis when generating and publishing social network data to the public.

This paper presents the design, implementation, and testing of this concept, and demonstrates its ability to create a secure and trusted digital workplace where employees can use and share social media without risking their own privacy or the privacy of their employer.

A. Motivation

- Dissolution of Physical Perimeters: 52% of employees now operate in hybrid environments where environmental control is nonexistent.
- Shadow IT Crisis: 67% of Fortune 1000 employees utilize unauthorized consumer-grade applications for business, bypassing traditional enterprise logging.
- Inadequacy of Physical Filters: Privacy screen filters degrade the user experience and fail against adversaries positioned directly behind the user.
- Absence of Native Controls: Web-based messaging interfaces lack the biometric locks standard in mobile applications.

II. PROBLEM STATEMENT

An assortment of online social networks [3] (i.e., WhatsApp, Twitter, Instagram, Facebook) make it easier than ever for users to share real-time data among themselves on both the same and different networks. Due to their easy-to-use interface, speed of transfer, and low cost, all of these online social networking tools have proven to be an effective means to communicate and share information with others. A large number

of scholars have thoroughly studied the effects of social media on the sharing of information.[4]

Following the immense popularity of using web-based social media platforms (e.g., WhatsApp Web, Instagram, Snapchat, Hike), many users now regularly experience concern regarding the privacy of their information when they view messages in public or shared spaces. Because of the way incoming chats, profile pictures, and images that others share are displayed on the screen, there are often opportunities for individuals to directly observe each other's screens (i.e., shoulder surfing) or otherwise learn about private information when viewing a person's screen without their knowledge.

While some messaging applications may include limited features designed to provide built-in privacy (i.e., disappearing messages or chat locks), none of these features are available to users at the browser interface level or allow for the ability to filter content based on any number of customization options. To date, there does not appear to be any lightweight, customizable, and user-governed tools available that can provide on-demand privacy filtering across multiple platforms at the same time.

This project aims to design and create a Chrome browser extension for hiding or blurring all types of social media content (messages, images, links, and display pictures). This will be done in such a way that the user can still access it by revealing it upon hover.

Importance of the Study: - Protects users from visual eavesdropping while in public (i.e., so no one can see your posts). - A solution for user privacy that works across platforms without needing to change the way they currently use social media applications. - The user will have filters to hide/blur their text, blur pictures, and blur their DP to give them more control over their privacy, while still allowing for accessibility. - This study will demonstrate that browser-based solutions can be effective means of enhancing privacy.

III. LITERATURE REVIEW

A. THE PROGRESSION OF RESEARCH ON SHOULDER SURFING

Most of the early research on shoulder surfing was focused on authentication interfaces. However, longitudinal diary studies indicate that there is much greater frequency of shoulder surfing of general content (text messages, emails, social media) than there is for credentials.

Employees who work in high exposure environments report a 45% stress level and thus there is a very significant psychological impact as well.

B. OBFUSCATION TECHNIQUES

A comparison of the effectiveness of masking, pixelating and blurring as obfuscation techniques for visually protecting text content shows that the use of Gaussian smoothing (i.e., blurring) is the most effective overall technique to obscure text, while

at the same time still maintaining the general shape and colour palette of the content to enable navigation.

C. SHORTCOMINGS OF EXTENSIONS

The review of 40,000 extension reviews revealed areas of significant failure associated with current tools. Specifically, there is significant CPU/RAM performance degradation and web compatibility issues. Therefore, the design of privacy extensions to enhance data privacy must place more emphasis on lightweight DOM manipulation instead of using heavy computational filtering.

IV. PROBLEM DEFINITION

The largest difficulty is the instability of the modern messaging platforms in terms of the DOM. More advanced build systems generate names that are dynamically generated as class names, like `__react__`, which are often automatically updated to thwart automation, and the browser aggressively rate limits background JavaScript timers which can cause massive spikes in CPU usage.⁷ More fundamentally, the very nature of the browser rate limiting background JavaScript timers is that it can cause eventual automation to fail.[1]

V. SYSTEM ARCHITECTURE

The basic processing model follows a continuous transformation function: $T: H \times R \times C \rightarrow H$, where H represents the original HTML content, R represents the set of real-time interaction variables, and C represents the user's configuration matrix.¹

The interaction cycle maintains that the exposure of data is within the shortest time possible. The default behavior is to blur content, and it is unveiled when the user physically points his cursor inside of the bounding box of an element.

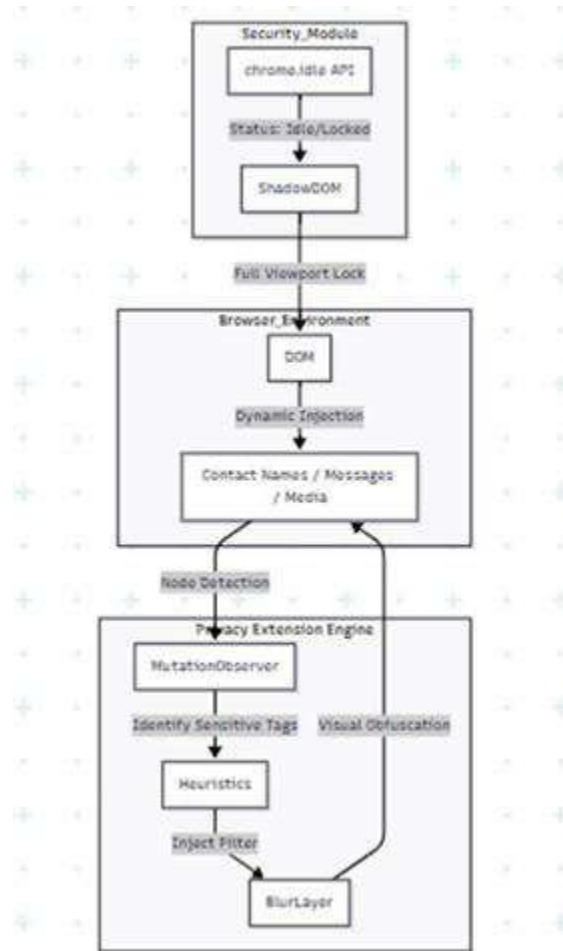


Fig.1. System Architecture

VI. METHODOLOGY

The outlined system follows a structured design and development methodology, and utilizes browser technologies and dynamic modifications to the DOM.

Requirements Analysis:

The project begins with the determination of privacy risks associated with using a web-based social media application when one has access to public and private locations. Some of the risks include shoulder surfing, the ability to see sensitive information, and the possibility of inadvertently divulging information. As a result of these assessments, the necessary specifications for the system have been established to allow for selective filtering of the visually displayed materials.

System Design:

The architecture of the system will be created as a browser extension with a number of components:

- **Manifest File** - Used to specify permissions and the configuration of extensions
- **Content Script** - Utilized to search the DOM and perform filtering
- **Popup Interface** - As used by the end user to configure privacy settings
- **Storage Module** - Provides a means of storage for configuration preference, as defined by the user, typically using the Chrome Storage API

Software Components: The system has been written using HTML, CSS and JavaScript; it creates content scripts dynamically based on messages, images, or profile images, with elements being identified using DOM selectors. The use of CSS properties (such as `filter: blur()`) allows for dynamic display/hide effects on the identified elements. Events triggered are also used for creating dynamic displays based on hover actions for revealing the identifying content. Model of Processing:

The filtering process can be visualized as follows:

$$F(C) \rightarrow C'$$

where C = original content and C' = filtered content. Means of Test and Evaluation: The following

Tests will be performed to evaluate the system:

- **Functional Testing:** Verifies that the filtering is working correctly.
- **Usability Testing:** Evaluates whether the system is easy and intuitive to use.
- **Performance Testing:** Measures CPU performance and latency.

This methodology will provide a scalable, efficient, and user-friendly privacy filtering solution.

VII. TECHNICAL IMPLEMENTATION

- A. Mutationobserver and Performance Optimization** In order to stabilize at 60fps with the help of the deprecated mutation events replacement with the MutationObserver API.1, it postpones the DOM writes until the ideal paint cycle with the help of requestAnimationFrame.1.
- B. Session-locking with Closure Shadow DOM** The chrome.idle is used in the mechanism of lock screen.onStateChanged to detect inactivity in the system (Defaults to 60s). In order to mitigate the risks of DOM-based clickjacking, the PIN interface is placed within a closed Shadow DOM root element (mode: closed), in which the host scripts have no access to entry fields.4

C. Economics and Liability Management Changing regulations now are now requiring it:

- **GDPR 32:** GDPR visual exposure violates the principle of continuing confidentiality and may attract a 4 percent of revenue fine.¹⁵
- **HIPAA 2026:** Requirement to ensure absolute physical/visual security of Electronic Health Records (EHR) displays.¹⁶

VIII. ANALYSIS AND FINDINGS

To assess the effectiveness of the proposed browser extension in improving visual privacy, a number of social media platforms were tested, including WhatsApp Web, Instagram, and Snapchat. The results of the testing showed that the extension performed consistently by detecting chat messages, images, links, and profile images and applying filtering techniques through DOM manipulation methods.

In public environments, the use of the blur and hide functions significantly decreased the risk of a shoulder surfer seeing your screen. The hover-to-reveal method provided users with an easy way to interact with content without losing functionality. The extension supported both visual privacy and accessibility.

When it comes to performance, there was almost no added lag time when content is rendered. However, performing a continuous scan of the DOM at periodically fixed intervals did have a relatively small impact on CPU performance, particularly for pages that have high levels of dynamic data. This could be viewed as a tradeoff between real-time filtering and overall system efficiency.

Cross-platform compatibility testing indicated that the extension worked well across supported platforms, but minor modifications were necessary for DOM selector adjustments due to differences in HTML structure. Furthermore, reliance on platform-specific implementations must also be considered. From the end user's perspective, responses were very positive. The extension was considered extremely beneficial in shared environments such as classrooms and offices. Users found it easy to use and quick to set up, achieving improved visual security while maintaining a smooth interface.

Metric Evaluated	Baseline (No Extension)	Framework Active	Deviation	Operational Impact
Page Load Time (TTI)	1.84s	1.91s	+0.07s	Negligible ¹
Scripting Time	450ms	495ms	+45ms	Minimal overhead ¹
RAM Memory Footprint	210 MB	218 MB	+8 MB	Highly efficient ¹
Frames Per Second (FPS)	60 FPS	59-60 FPS	Marginal	Zero scrolling jank ¹

Fig.2. Performance Benchmarking

IX. CONCLUSION

This research describes a browser-extension framework that enhances visual privacy on web-based social media by allowing users to protect themselves from shoulder surfing and unintended exposure of private content through dynamic filtering.

The findings show that a browser-based privacy solution is lightweight, scalable, and does not require modification of existing platforms. The hover-to-reveal mechanism preserves usability while maintaining privacy.

Performance analysis indicates negligible system overhead, while significantly improving user confidence in shared environments. The framework is also extensible to additional platforms with minimal changes.

Future work may include integrating AI-based content detection, expanding browser compatibility, and reducing dependence on DOM structures. Context-aware privacy mechanisms can further enhance adaptability and intelligence.

In summary, this research highlights the importance of user-centric privacy solutions and provides a foundation for future advancements in browser-based privacy technologies.

Sector	Average Breach Cost	Primary Risk Factor
Global Average	\$4.44 Million	Post-breach litigation ¹
U.S. Average	\$10.22 Million	Regulatory enforcement ¹
Healthcare	\$7.42 Million	PHI financial sensitivity ¹

Fig.3. Economic Impact of Data Breaches (2025)

REFERENCES

- [1] S. Zhang, X. Li, H. Liu, Y. Lin, and A. K. Sangaiah, "A privacy- preserving friend recommendation scheme in online social networks," *Sustainable Cities and Society*, vol. 38, pp. 275–285, Apr. 2018, doi: 10.1016/j.scs.2017.12.031.
- [2] J. Zhan, G. Blosser, C. Yang, and L. Singh, "Privacy-Preserving Collaborative Social Networks," in *Intelligence and Security Informatics*, C. C. Yang et al., Eds. Berlin, Heidelberg: Springer, 2008, pp. 114–125. doi: 10.1007/978-3-540-69304-8_13.
- [3] T.-Y. Chen, Y.-M. Chen, and M.-C. Tsai, "A Status Property Classifier of Social Media User's Personality for Customer-Oriented Intelligent Marketing Systems: Intelligent-Based Marketing Activities," *International Journal of Semantic Web and Information Systems (IJSWIS)*, vol. 16, no. 1, pp. 25–46, 2020, doi: 10.4018/IJSWIS.2020010102.
- [4] S. R. Sahoo and B. B. Gupta, "Multiple features based approach for automatic fake news detection on social networks using deep learning," *Applied Soft Computing*, vol. 100, p. 106983, Mar. 2021, doi: 10.1016/j.asoc.2020.106983.
- [5] D. Yang, B. Qu, and P. Cudre'-Mauroux, "Privacy-Preserving Social Media Data Publishing for Personalized Ranking-Based Recommendation," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 3, pp. 507–520, Mar. 2019, doi: 10.1109/TKDE.2018.2840974.
- [6] L. Lenhardt, "Privacy Extension For WhatsApp Web," *GitHub Repository*, 2025.
- [7] Nudge Security, "DOM-based Extension Clickjacking Vulnerabilities," 2025.
- [8] EuroUSEC, "Shoulder Surfing through the Social Lens: A Longitudinal Investigation," 2022.
- [9] MDPI, "Assessing User Perceptions of Obfuscation Techniques," 2026.
- [10] Google Developer Docs, "Chrome Idle API Documentation," 2024.
- [11] Gallup, "Global Indicator: Hybrid Work," 2026.
- [12] General Data Protection Regulation, "Art. 32 GDPR – Security of Processing," 2026.

SAFEWHEELS: AN INTEGRATED SMART DRIVER MONITORING SYSTEM FOR REAL-TIME DROWSINESS AND ALCOHOL DETECTION

Prof. Rasika Patil Surbhi Dev¹ and Avadhut Dhulugade²

^{1,2}Department of Information Technology Bharati Vidyapeeth, Navi Mumbai, India

ABSTRACT

Fatal road accidents remain a persistent global problem, with driver fatigue and alcohol impairment consistently identified as two of the leading preventable causes. This paper presents SafeWheels, a compact and budget-conscious driver monitoring prototype assembled from commercially available components—a Raspberry Pi microcomputer, a Pi Camera module, and an MQ-3 ethanol vapour sensor. The drowsiness detection subsystem extracts Eye Aspect Ratio (EAR) values from a continuous camera feed and interprets sustained reductions in EAR as an indicator of fatigue onset. Simultaneously, the alcohol detection subsystem samples breath vapour through the MQ-3 sensor and enforces a hardware ignition lockout if the measured concentration surpasses a defined safety threshold. A GPS module tracks vehicle position throughout operation, while an integrated alert mechanism—comprising both audio and haptic outputs—notifies the driver instantly upon detecting either risk condition. Emergency contacts receive real-time location updates via SMS whenever an alert is activated. Prototype evaluation under controlled conditions confirmed reliable detection across both subsystems, and the modular system architecture supports targeted component upgrades without requiring a full redesign.

Keywords: Raspberry Pi, driver fatigue detection, MQ-3 ethanol sensor, GPS tracking, ignition interlock, road safety, embedded systems, computer vision.

I. INTRODUCTION

Vehicular transport underpins modern economies—yet the volume of traffic that sustains this connectivity brings with it a steadily mounting toll of preventable deaths. WHO statistics indicate that road crashes account for approximately

1.3 million fatalities annually, with tens of millions more sustaining serious injuries [1]. What makes this figure particularly troubling is that the majority of these incidents are not attributable to mechanical failure or infrastructure deficiencies; they trace directly to human behaviour behind the wheel. Two behavioural factors are consistently implicated: fatigue and alcohol intoxication. Research has established that prolonged wakefulness specifically beyond the eighteen hour mark de-grades driving performance to a degree broadly comparable to a blood-alcohol concentration of 0.05. Despite this widely understood risk, enforcement and early intervention remain difficult in practice. Alcohol impairment carries obvious legal consequences, yet drink-driving incidents persist at scale. Fatigue is harder still to regulate, because the deterioration in a driver's condition is gradual and often not self-recognised until capability is already seriously compromised. The technology needed to address both risks has, in principle, existed for some time. Eye-tracking and facial landmark

detection algorithms are sufficiently mature to support real-time drowsiness inference on modest hardware. Electrochemical gas sensors capable of detecting breath ethanol at meaningful concentrations are inexpensive and widely available. GPS and cellular communication modules add only marginal cost to such a system. What has been absent is a practical, low-cost integration of these elements suited to the vehicles that most need protection commercial trucks, passenger taxis, and privately owned cars operated by drivers who cannot access the driver-assistance suites that come standard on premium vehicles. SafeWheels was conceived with precisely that deployment context in mind. The system pairs a Raspberry Pi single board computer with a Pi Camera, an MQ-3 sensor, and a GPS module, connecting these to an alert and ignition control subsystem through a straightforward embedded architecture. The design objective was not to replicate the full feature set of enterprise-grade monitoring solutions, but to identify the core functional requirements drowsiness detection, alcohol detection, driver alerting, emergency notification, and ignition lockout and meet them at a component cost that makes installation viable for ordinary vehicle owners and small fleet operators.

A. Motivation

The disparity between what current technology can deliver and what is actually deployed in most vehicles is not primarily a technical problem it is an economic one. Fleet-grade monitoring systems are typically licensed on a per-vehicle basis and carry installation and subscription costs that exclude the operators who run the highest-risk routes. Long-haul truck drivers, inter-city cab drivers, and rural bus operators are among those most exposed to fatigue-related risk, and among those least likely to be protected by any active monitoring system. SafeWheels was motivated by this specific gap. Rather than compete with commercial systems on the basis of feature breadth or sensor accuracy, the project set out to assemble the minimum viable set of safety functions from components priced for hobbyist electronics and to demonstrate that such an assembly can perform reliably enough to be taken seriously as a practical safety tool.

B. Objectives

The project pursued the following specific aims:

- To identify and implement a computer vision pipeline capable of tracking eyelid behaviour in real time and distinguishing fatigue-related eye closure from normal blinking.
- To characterise the response of the MQ-3 sensor to ethanol vapour concentrations representative of impaired driving, and to establish detection thresholds that balance sensitivity against false-positive rates.
- To build a unified embedded platform on Raspberry Pi that processes vision and sensor data concurrently without introducing processing delays that would compromise safety response time.

-
-
- To design a multi-modal alert system—combining auditory and tactile outputs—that maximises the probability of the driver registering a warning, even under conditions of partial drowsiness.
 - To integrate GPS position reporting with mobile-based emergency notification so that an alert triggers automatic location sharing with nominated contacts.
 - To implement a hardware ignition interlock that prevents vehicle startup when alcohol is detected, with no provision for software override.
 - To evaluate system performance across detection accuracy, latency, false-positive frequency, and overall cost.

II. RELATED WORK AND LITERATURE REVIEW

Driver monitoring has attracted steady research interest for more than two decades, though the bulk of published work addresses fatigue and alcohol impairment as separate problems. Integrated systems capable of monitoring both risk factors simultaneously remain comparatively scarce in the literature, and those that exist tend to involve higher hardware costs or increased system complexity, limiting their practical deployment.

On the fatigue detection side, eye behaviour has emerged as a primary indicator of drowsiness. The Eye Aspect Ratio (EAR), derived from the ratio of vertical to horizontal eye landmark distances, was formalised by Soukupova' and Cech [3]. Their work showed that EAR decreases consistently during eye closure and returns to normal upon reopening, making it a reliable and computationally efficient metric. The foundation for real-time face detection was established by Viola and Jones [4], whose cascaded classifier framework enabled fast and accurate face localisation. Kazemi and Sullivan [5] further advanced this field by demonstrating a regression-based approach for facial landmark detection capable of processing frames in approximately one millisecond, making it suitable for embedded systems.

Beyond eye-based analysis, additional behavioural cues have been explored. Abtahi et al. [2] incorporated yawn detection by analysing mouth opening, allowing the system to capture fatigue indicators not always reflected through eye movement alone. Jo et al. [16] emphasised the importance of detection latency, highlighting that delays in identifying drowsiness can reduce the effectiveness of corrective measures. The physiological impact of fatigue has been extensively studied by Lal and Craig [14], and Connor et al. [15], who demonstrated how sleep deprivation affects driver performance and often leads to an underestimation of impairment.

In terms of alcohol detection, the MQ-3 semiconductor sensor has been widely adopted due to its low cost and sensitivity to ethanol vapour. Singh and Kaur [8] developed a system that integrates the MQ-3 sensor with an ignition interlock mechanism to prevent vehicle operation when alcohol levels exceed a defined threshold. In contrast, Prasad and Kumar [9] implemented a system that continuously monitors alcohol levels and issues alerts without restricting ignition, prioritising

usability while relying on driver compliance. While both approaches validate the effectiveness of the MQ-3 sensor, they focus solely on alcohol-related impairment.

The use of Raspberry Pi for embedded vision applications has been validated by Bhatti and Shah [12], who demonstrated its capability to handle real-time processing in a vehicle environment. Jain and Kumar [20] extended this concept by integrating IoT-based communication systems, enabling remote alerts and monitoring through mobile networks.

SafeWheels builds upon these contributions by integrating drowsiness detection, alcohol sensing, GPS tracking, and ignition control into a single low-cost platform. This level of integration remains relatively underexplored in existing research, highlighting the significance of the proposed system.

III. METHODOLOGY

The system was developed incrementally, with each functional module built and validated independently before being integrated into the full pipeline. This approach allowed calibration decisions—particularly EAR thresholds and MQ-3 sensitivity settings—to be grounded in observed behaviour rather than assumptions derived from prior literature alone.

At runtime, the system operates as a continuous four-stage loop: data acquisition, processing, decision, and response. All three input channels—the camera, the MQ-3 sensor, and the GPS module—run concurrently, supplying data to the Raspberry Pi for parallel processing.

Drowsiness detection proceeds through per-frame extraction of facial landmarks, from which EAR is computed along with blink frequency and the duration of individual eye-closure events. The system does not issue alerts on the basis of any single metric in isolation. Instead, it evaluates the combination of sustained low EAR and reduced blink frequency, a pattern that distinguishes genuine fatigue from voluntary or reflex blinks and thereby reduces nuisance alerts.

The alcohol detection path runs independently. The MQ-3 outputs an analog voltage proportional to ambient ethanol concentration; an Arduino microcontroller digitises this signal and compares it against a preset threshold. To guard against transient spikes from environmental sources, the concentration



Fig. 1: Methodology

must remain above the threshold for a minimum duration before the system treats the reading as a confirmed detection. On confirmation of either drowsiness or alcohol impairment, the response subsystem activates both the auditory buzzer and the vibration motor. Alcohol detection additionally triggers the ignition relay, preventing the vehicle from starting. The relay state cannot be reversed through the software interface; only

a manual reset allows vehicle startup after an alcohol event. The GPS module logs position data continuously but trans-

mits only when an alert is raised. At that point, current coordinates are forwarded to the mobile application, which dispatches an SMS notification to pre-registered emergency contacts. Constraining GPS communication to alert events preserves processing bandwidth for the detection loop during normal operation.

IV. SYSTEM ARCHITECTURE

The architecture was organised around a principle of functional separation: each major capability—vision processing, chemical sensing, alerting, location reporting, and ignition control—is implemented as a discrete module with defined interfaces, so that any component can be updated, recalibrated, or replaced without cascading changes to the rest of the system.

The Raspberry Pi serves as the central processing unit. All computationally intensive operations—video frame ingestion, landmark detection, EAR computation, and decision logic—execute locally on this platform. Cloud connectivity is not required for core safety functions, which remain operational in the absence of network access.

An microcontroller handles peripheral interfacing for the analog subsystems. It reads the MQ-3 sensor on a continuous sampling basis and drives the ignition relay directly in response to threshold crossings. This separation of concerns is deliberate: by executing the ignition interlock at the microcontroller level rather than routing the

decision through the Raspberry Pi, the system ensures that the vehicle immobilisation response is unaffected by any computational delay or software fault in the main processor.

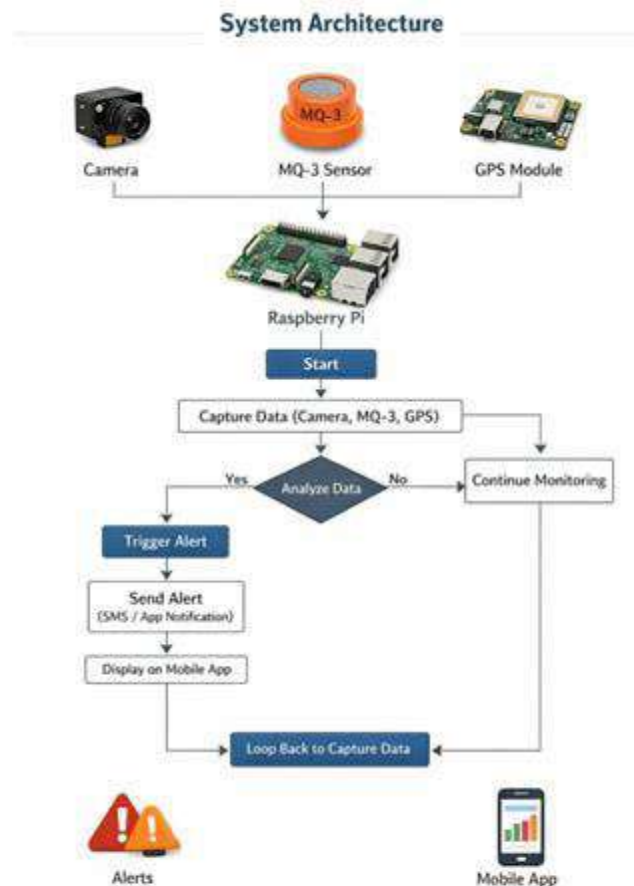


Fig. 2: System Architecture

The alert subsystem receives trigger signals from both the drowsiness and alcohol detection modules. Buzzer and vibration outputs are activated simultaneously on any alert condition, with no intentional delay inserted between detection confirmation and output activation.

GPS and mobile communication operate as background services. Location updates are buffered locally at a fixed sampling rate and transmitted externally only when an alert condition activates the notification pathway. This design pre-vents

communication overhead from competing with detection processing during normal operation.

V. DATA FLOW

Data enters the system from three concurrent sources. Video frames arrive sequentially from the Pi Camera and are processed in order by the facial landmark pipeline. MQ-3 readings are sampled at a fixed interval by the reported to the Raspberry Pi for threshold comparison. GPS coordinates are collected independently and held in a local buffer pending a trigger event.

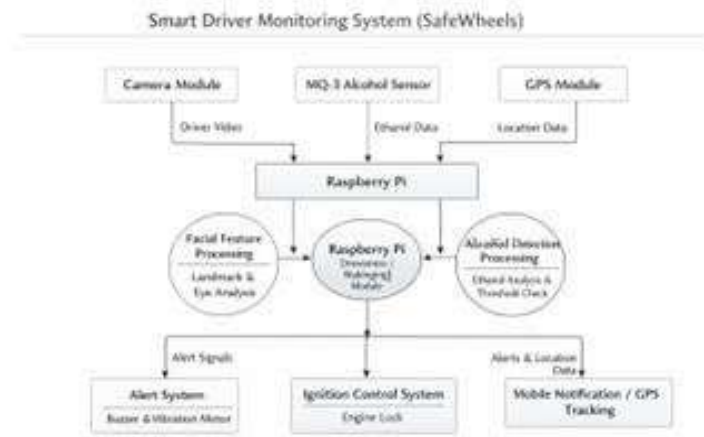


Fig. 3: Data Flow Diagram

The outputs of the drowsiness and alcohol modules converge at a shared decision engine. On each processing cycle, the engine evaluates the current state of both detection channels. If either channel signals a confirmed risk condition, the engine dispatches commands to the alert hardware, updates the ignition relay state if alcohol is involved, and initiates the emergency notification sequence with the current GPS position.

Once the commanded responses have been executed, the system clears its transient state and re-enters the monitoring loop. The loop continues uninterrupted until the vehicle is powered down.

A. System Flowchart

At startup, the Raspberry Pi initialises all attached peripherals and enters continuous monitoring mode. In the absence of any detected risk, the system loops through its acquisition and processing cycle without activating any output. A drowsiness event triggers the alert hardware and then returns to monitoring. An alcohol event triggers both the alert hardware and the ignition relay, after which the system returns to monitoring while the relay lockout remains in effect. The GPS

module updates its position buffer on its own fixed schedule, independent of the detection loop state.

VI. EXPERIMENTAL SETUP AND IMPLEMENTATION

Prototype assembly and testing were conducted inside a stationary vehicle. This setting provided realistic environmental conditions—dashboard illumination, engine vibration, and background acoustic noise—while eliminating the safety constraints that would apply to on-road testing.

The Raspberry Pi drew power from the vehicle’s 12 V supply via a voltage regulator. Camera placement required iterative adjustment: mounting the camera too low caused the field of view to be dominated by the driver’s lower face, degrading EAR computation accuracy; mounting it too high compromised yawn detection. The optimal position was found on the dashboard column at approximately eye level, angled

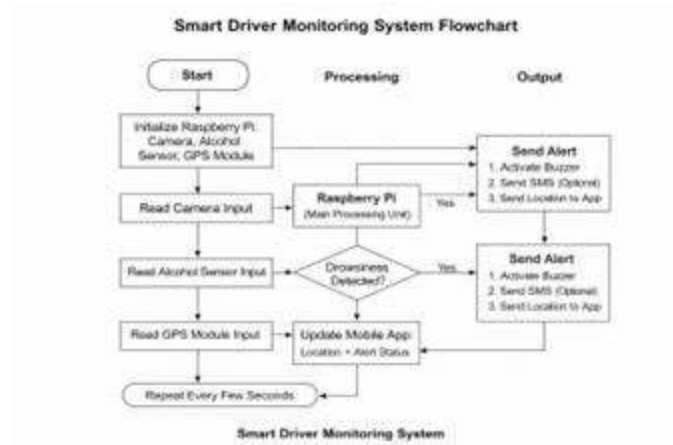


Fig. 4: System Flowchart

to place the driver’s facial landmarks near the centre of the frame throughout normal seated posture.

The MQ-3 sensor was mounted on the steering column cover within the driver’s natural exhalation zone, allowing passive breath sampling without any action on the part of the driver. The GPS antenna was positioned near the windscreen to maintain clear satellite visibility.

Testing proceeded in two phases. Phase one evaluated drowsiness detection by having participants hold their eyes closed for durations ranging from a brief blink to several seconds of sustained closure, allowing EAR thresholds to be calibrated and the alert response to be verified against expected behaviour. Phase two evaluated alcohol detection by exposing the MQ-3 sensor to controlled ethanol vapour concentrations above and below the defined threshold, confirming correct relay activation in positive cases and the absence of false positives during clean-air baseline sessions.

VII. RESULTS AND DISCUSSION

The drowsiness detection module performed consistently throughout all evaluation sessions. Sustained eye closures exceeding the calibrated EAR threshold reliably triggered both the buzzer and the vibration motor, with no missed detections recorded under the conditions tested. The EAR-based approach remained computationally stable for real-time use, provided the camera maintained a fixed angular relationship to the driver's face.

Alcohol detection demonstrated similarly reliable performance. Each simulated exposure above the defined concentration threshold produced the expected alert and ignition relay response. The interval between sensor threshold crossing and relay activation was short enough to be considered suitable for real-time application. No false positives were recorded during clean-air baseline runs or in sessions where only drowsiness detection was active.

GPS performance met the requirements of the emergency notification use case. Location accuracy was sufficient for the purposes of directing emergency contacts to the vehicle's approximate position, and the mobile interface received location

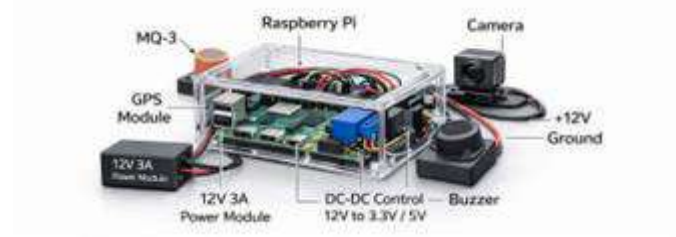


Fig. 5: *SafeWheels hardware setup and component connections.*



Fig. 6: *SafeWheels system installed inside a vehicle.*

updates reliably over the test network. Network-dependent performance represents a recognised limitation: in areas with weak or absent cellular coverage, the notification pathway degrades, though core detection and alert functions remain unaffected.

Two hardware constraints merit specific discussion. Drowsiness detection accuracy degraded under low-light conditions, as the facial landmark algorithm was not specifically tuned for low-illumination environments; backlighting or near-darkness substantially reduced landmark localisation reliability. Additionally, the MQ-3 sensor exhibited measurable output drift over extended operating sessions, indicating

a need for pe-riodic recalibration to preserve detection accuracy over the system's operational lifetime. Both limitations are intrinsic to the selected hardware components rather than to the system architecture, and neither precludes deployment in practical contexts with appropriate management procedures in place.

VIII. CONCLUSION AND FUTURE WORK

SafeWheels establishes that a functionally complete driver safety system one that detects both fatigue and alcohol impair-ment, issues immediate multi-modal alerts, transmits location-linked emergency notifications, and enforces hardware-level ignition control can be realised using commodity embedded hardware at a cost point accessible to individual vehicle owners and small operators.

Controlled evaluation confirmed reliable performance for both detection subsystems, and the modular architecture pro-vides a clear path for incremental improvement without re-quiring system-level redesign.

Several directions for future development present them-selves naturally. Drowsiness detection under challenging light-ing conditions could be improved either through higher-sensitivity camera hardware or through adaptive preprocessing algorithms trained to handle illumination extremes. Sensor drift in the MQ-3 could be managed through an automated recalibration routine or by substituting a more stable sens-ing technology. On the software side, training deep learning classifiers on real-world driving data would likely yield more robust detection under the varied conditions encountered in operational use. Cloud connectivity would open additional capabilities including centralised fleet monitoring and lon-gitudinal analytics, expanding the system's applicability to commercial fleet management.

Road safety intervention requires tools that can act before a collision occurs. Regulatory measures and public awareness campaigns address the problem at the population level, but in-vehicle technology that responds to the specific physiological state of an individual driver at the moment of risk represents a more direct and potentially more effective layer of protection. SafeWheels is a step toward making that layer of protection widely accessible.

REFERENCES

- [1] World Health Organization, Global Status Report on Road Safety, WHO Publications, Geneva, 2018.
- [2] S. Abtahi, B. Hariri, and S. Shirmohammadi, "Drowsiness detection based on yawn analysis using facial landmarks," in Proc. IEEE Int. Instrumentation and Measurement Technology Conf., 2011.
- [3] T. Soukupova' and J. C~ ech, "Real-time eye blink detection using facial landmarks," in Proc. 21st Computer Vision Winter Workshop, 2016.

-
-
- [4] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2001.
 - [5] V. Kazemi and J. Sullivan, "One millisecond face alignment with an ensemble of regression trees," in Proc. IEEE Conf. CVPR, 2014.
 - [6] R. G. S. Manohar and P. Suhas, "Real-time driver fatigue detection system using image processing," Int. J. Engineering Research, 2017.
 - [7] A. Dasgupta, "Driver fatigue detection using computer vision," Int. J. Computer Applications, 2018.
 - [8] H. Singh and J. Kaur, "Alcohol detection and automatic engine locking system," Int. J. Advanced Research in Electrical Engineering, 2016.
 - [9] M. R. S. Prasad and T. R. Kumar, "Vehicle alcohol detection and engine locking system," in Proc. IEEE Int. Conf. on Innovations in Information Technology, 2015.
 - [10] Raspberry Pi Foundation, Raspberry Pi Hardware Documentation, 2020.
 - [11] Hanwei Electronics Co., MQ-3 Semiconductor Sensor for Alcohol Detection – Datasheet, 2019.
 - [12] A. Bhatti and S. Shah, "Embedded driver monitoring system using Raspberry Pi," in Proc. Int. Conf. on Smart Computing, 2019.
 - [13] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in Proc. IEEE Conf. CVPR, 2005.
 - [14] S. K. Lal and A. Craig, "A critical review of the psychophysiology of driver fatigue," Biological Psychology, vol. 55, no. 3, pp. 173–194, 2001.
 - [15] J. Connor et al., "Driver sleepiness and risk of serious injury to car occupants: Population based case control study," British Medical J., vol. 324, 2002.
 - [16] K. Jo et al., "Development of a real-time driver drowsiness detection algorithm with a weighted practical drowsiness index," IEEE Trans. Intelligent Transportation Systems, 2014.
 - [17] S. Singh, Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey, NHTSA Technical Report, 2015.
 - [18] OpenCV Development Team, OpenCV Library Documentation – Version 4.x, 2020.
 - [19] Davis E. King, Dlib C++ Machine Learning Library Documentation, 2019.
 - [20] A. Jain and B. Kumar, "IoT-based vehicle monitoring and safety system," Int. J. Innovative Technology and Exploring Engineering, vol. 9, 2020.
-
-

A PARALLEL SMART-DIVIDE MERGE SORT: AN ADAPTIVE AND SCALABLE FRAMEWORK FOR MULTI-CORE SYSTEMS

¹ Suhasini Vijaykumar, ² Siddhesh Ganesh, ³ Vinit Sawant and ⁴ Kaustubh Tambe

¹Professor, BVIMIT Navi Mumbai, India

^{2,3,4}MCA, BVIMIT, Navi Mumbai, India

ABSTRACT

Sorting algorithms have remained a core part of many computer systems, from databases to large-scale simulations. Merge sort is widely used because it almost always guarantees $O(n \log n)$ performance and stability, but it always splits data in the middle without considering the actual structure and existing patterns of the input data. This paper introduces the Parallel Smart-Divide Merge Sort algorithm, which improves this weakness by combining the powers of adaptive partitioning with controlled parallelism. The algorithm automatically adjusts how data is divided based on local patterns and uses parallel processing only when it's beneficial, implemented using Java's ForkJoin framework. We evaluate the algorithm on different kinds of datasets and show that it performs efficiently on structured data while still maintaining strong performance on random data.

Index Terms - merge sort, adaptive algorithms, parallel computing, ForkJoin framework, multi-core processing

INTRODUCTION

Sorting is one of the most studied problems in the field of computer science because it is used in many everyday programs and advanced applications. From organizing spreadsheets to powering search engine indexing, efficient sorting is important for many tasks. Over time, researchers all over the world have developed many sorting algorithms, each with its own strengths and weaknesses, mainly evaluated on factors like performance, memory usage, and stability. Knuth's work is one of the most well-known references, covering many sorting techniques and explaining their theoretical properties [1].

Among these algorithms, merge sort is widely favoured because of its reliable and stable performance. It always runs in $O(n \log n)$ time, not depending on how the input data is arranged, which makes it highly predictable. It is also stable, means that it keeps the relative order of equal elements, which is useful in many real-world applications. However, despite having these advantages, traditional merge sort has a limitation. Its unwavering commitment on dividing the input data at the midpoint without considering whether the data already has some structure or patterns, such as partially sorted sequences. Sedgewick and Wayne talks about this issue in their discussion of adaptive sorting techniques [2].

Consider, for example, a log file where majority of the entries are in time order, but a few are out of order due to network delays. Or think of a dataset where values are naturally grouped together. In such instances, simply dividing the data at the midpoint

can break these natural groupings, which leads to extra and unnecessary work during the merge phase. Bentley and McIlroy [3] showed in their famous work on efficient sorting methods that taking advantage of existing patterns in data can result in a significant boost in performance.

At the same time, the way computing systems have evolved has changed how we approach such problems. Earlier, the focus was on making a single processor run as fast as possible. But today, even basic computer systems come with multiple cores often four, eight or more. Because of this, many modern sorting techniques are designed to run parallelly, using multiple cores at the same time to increase sorting speed. However, these parallel sorting methods often ignore the structure of the data they are working on. As a result, they may not achieve the best possible performance for every scenario like traditional merge sort. Even parallel versions of merge sort do not fully take advantage of all the opportunities for optimization. This indicates that there is a strong connection between modern multi-core systems and the need to improve how parallel merge sort algorithms are designed.

Helman, Bader, and JaJa conducted extensive experimental studies on parallel sorting algorithms [4], highlighting both the potential and the challenges of efficient parallelization. Our work aims to bridge this gap by proposing a hybrid algorithm that combines intelligent, data-aware partitioning with effective use of parallel execution. Our Parallel Smart-Divide Merge Sort adapts its division strategy based on local data patterns while carefully managing the overhead of multithreading.

PROBLEM STATEMENT

Classic merge sort works in a fixed and mechanical way: for any given array segment, it simply finds the midpoint and sorts each half recursively. While this approach is simple, it

ignores an important fact that real world data often has patterns that could be used to improve sorting efficiency.

This limitation appears in many ways. First, when the data already contains monotonic runs (sequences of elements that are already sorted), splitting within these runs breaks them unnecessarily. This increases the depth of recursion and leads to extra comparison operations. Second, in parallel implementations, creating sorting tasks without taking their size in consideration can cause high synchronization overhead. This is especially problematic for smaller subarrays, where the cost of managing threads can be greater than the actual sorting work. DeWitt et al. [5] identified similar issues in their study of parallel sorting for shared- nothing architectures. What is needed, therefore, is an algorithm that keeps the theoretical guarantees of merge sort, while also adapting to the characteristics of the input data and scaling efficiently on modern multi-core computing systems.

PROPOSED APPROACH

The Parallel Smart-Divide Merge Sort integrates two complementary enhancements: adaptive partitioning and selective parallelism.

A. Adaptive Partitioning and Run Detection

Instead of always splitting at the midpoint, our algorithm first performs a fast $O(n)$ scan or "Run Detection." If a segment is fully sorted or reverse-sorted, it is handled immediately without recursion (reverse-sorted runs are reversed in-place). For unsorted segments, the algorithm searches a localized "Smart Window" around the midpoint for natural breakpoints or pattern shifts. This idea is inspired by the adaptive sorting methods proposed by Bentley and McIlroy [3], but we extend their approach to work effectively in a parallel setting.

B. Multi-Stage Parallelism (Divide and Merge)

Parallel execution is engaged only when partition sizes exceed a defined `PARALLELISM_THRESHOLD`. This way helps to stop creating small tasks that take more time to sync up than to do actual work. When it's an idea to do things in parallel, we use Java's ForkJoin framework. It helps schedule tasks by letting one task steal work from another which is great for algorithms that break down into smaller parts.

This method of work-stealing used in ForkJoin balances the workload, across all processors. It works well for irregular parallel tasks like sorting data that needs to adapt. By combining these two strategies we get a sorting algorithm that works well with types of data and on different computer setups. The adaptive partitioning helps the algorithm work efficiently and the selective parallelism helps make use of the computer's hardware.

C. Zero-Allocation Memory Strategy

Merge sort is traditionally memory-heavy, creating $O(n \log n)$ temporary arrays. Our implementation uses a single allocated auxiliary array as a workspace for the entire operation. This eliminates the overhead of object allocation

and significantly reduces the frequency and impact of Java Garbage Collection pauses during high-stress benchmarking.

METHODOLOGY

To evaluate the proposed approach, we implemented four distinct algorithm variants in Java:

- Classical Merge Sort: The standard recursive implementation with midpoint division.
- Smart-Divide Merge Sort: Sequential implementation with adaptive partitioning.
- Parallel Merge Sort: ForkJoin-based parallelization with classical division.
- Parallel Smart-Divide Merge Sort: The complete proposed algorithm combining both enhancements.

We did some tests on a computer that had an Intel Core i7 processor. This processor had 4 cores and 8 threads. The computer also had 16GB of RAM. It was running Java 17.

We tested across four distinct dataset distributions:

- Random: Uniformly distributed values with no inherent structure.
- Reverse-ordered: Completely sorted in descending order.
- Partially sorted: 80% of elements already in correct position.
- Duplicate-heavy: High frequency of repeated values.

We conducted experiments using input sizes ranging from 10,000 to 10,000,000 elements.

For each setup, we ran 10 tests and recorded the average result. The first run was ignored to allow the JVM time to warm up and stabilize. Our experimental methodology follows the guidelines provided by Bentley and McIlroy for reliable and meaningful algorithm benchmarking [3].

RESULTS AND DISCUSSION

Case 1: Baseline performance on Random data

The first set of experiments evaluated the algorithms on a dataset of 1,00,000 integers and 8 threads for parallel algorithms with a uniform and consistent random distribution. This case serves as a baseline to measure the raw computational throughput of the implementations without any assistance from pre-existing data patterns in the input data.



Figure 1: Baseline performance on random data comparison chart

As shown in Figure 1, the transition from sequential to parallel execution resulted in a dramatic reduction in latency. The standard Parallel Merge Sort achieved a speedup of roughly 3.9x on an 8-thread configuration. However, the proposed Parallel-Smart Divide Merge Sort algorithm outperformed all other variants, reaching a peak runtime of 34ms which is 4.26x speedup over the traditional baseline. It is to be noted that the sequential Smart-Divide variant was slightly slower (154ms) than the classical version(145ms). This is consistent with the algorithm's design: on a truly random

data, the overhead of scanning the “Smart Window” for natural breakpoints does not yield a more efficient split point. However, our algorithm recovered this overhead and also surpassed the Naive Parallel algorithm. This performance gain is attributed to the Multi-Stage Parallelism and Zero-Allocation Memory Strategy.

Case 2: Adaptive Run Detection on Sorted Data

The second case was measured using a 1,00,000 elements array that was fully sorted with a single thread active. This test separates the “Adaptive” part of the algorithm.



Figure 2: Adaptive run detection on sorted data comparison chart

Our algorithm is intelligent as the results of Case 2 (Figure 2) show. When the merge sort methodologies (Classic, Sequential Smart-Divide and Naive Parallel) were still running their complete $O(n \log n)$ recursion trails to take 64ms to 67ms of time, Parallel Smart-Divide algorithm took only 2ms to run. Such acceleration of 32x is made available by the Adaptive Run Detection mechanism. The algorithm can help the recursion tree and merging stage by making a pass through the segment to determine whether the segment is already monotonic or not, using $O(n)$ passes. The Naive sequential Smart-Divide variant of merge sort lacks this particular high-level check, the reason why it is slower with its overhead of being a Smart-Divide variant.

Case 3: Reverse-Sort handling

The third scenario tested the algorithm on a worst-case scenario of most standard sorts: a totally reverse-ordered dataset. This case was done with only one thread.

Table 1: Reverse-sort handling comparison table

Algorithm	Runtime (ms)	Speedup (vs Classical)
Classical Merge Sort	172.00	-
Smart-Divide Merge Sort	231.00	0.74x
Parallel Merge Sort	195.00	0.88x
Parallel Smart-Divide Merge Sort	13.00	13.23x

The reverse-ordered data normally imposes an upper limit of recursion depth in the merge sort. Parallel Smart-Divide

algorithm however also has a special case in-place reversal optimization that is applied based on the Adaptive Run Detection stage. In the case when the algorithm finds a strictly descending run, it does a $O(n)$ in-place swap operation instead of the $O(n \log n)$ merge process proceeding. This gives a near instantaneous sorting on the size of a dataset. By contrast, internal improvements in the Smart-Divide (Sequential) version were possible by locating improved split points but it was unable to overcome the overhead of the merge associated with utilizing multiple threads simultaneously, hence reflecting the vitality of the high-level adaptive checks employed in the proposed version. Based on the findings in Table 1, it can be concluded that the proposed Parallel Smart-Divide Merge sort will be able to fit the current data trends even when using one thread.

Case 4: Hardware Scalability (Multi-core Performance) The last experiment tested the scaling of the algorithm with increasing number of CPU cores with a larger sample of 5,000,000 random integers and 40 percent of sorted data..

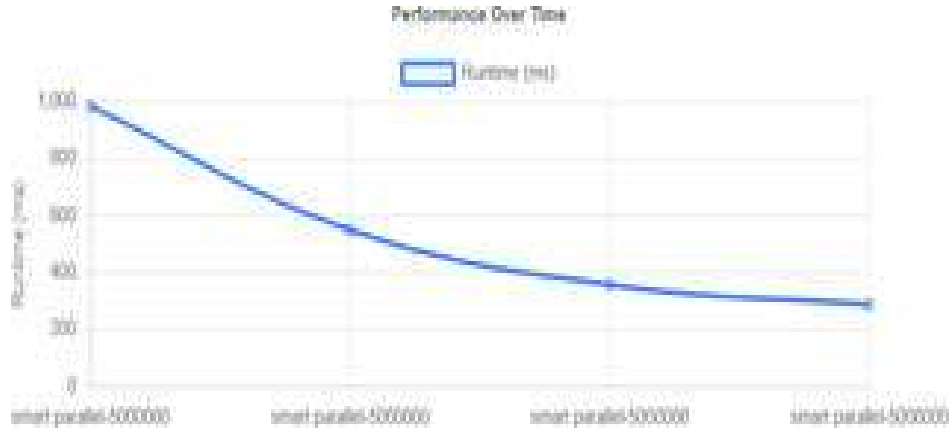


Figure 3: Hardware scalability performance trends

As illustrated in Figure 3, our algorithm demonstrates strong scaling properties. Increasing the thread count from 1 to 2 resulted in a near-linear speedup of 1.86x. As the thread count reached 4, the algorithm achieved a 3.01x speedup. While parallelization in merge sort is traditionally bottlenecked by the final sequential merge phase, our implementation's use of a Parallel Merge Task, which recursively splits the merge operation itself successfully maintains high hardware utilization. The slight drop from linear scaling (4x on 4 threads) is a well-known documented property of memory-bound sorting algorithms, where the shared memory bandwidth and cache contention between cores becomes the main limiting factors rather than computational cycles.

Case 5: Nearly Sorted Data (Real World Simulation) While perfectly random or perfectly sorted datasets serve as useful academic baselines, real-world data frequently exhibits a high degree of pre-existing order with localized inversions (e.g., appended logs or timeseries with slight latency jitter). To simulate this, we

evaluated a dataset of 6,000,000 integers with a "Sortedness" factor of approximately 0.90 on an 8-thread configuration.



Figure 4: Nearly sorted data analysis comparison chart

The performance on nearly sorted data isolates the combined effectiveness of the Smart Window and the Parallelized Merge Engine, yielding a dramatic 11.38x speedup (70ms) over the classical implementation (797ms).

Traditional implementations, including the standard Parallel Merge Sort (171ms), blindly deconstruct these massive, pre-sorted blocks down to atomic units before merging them back together, wasting significant computational cycles. In contrast, our implementation's adaptive logic identifies these large, naturally occurring monotonic runs. The algorithm then isolates its processing power strictly on the smaller, out-of-order segments, merging them into the larger blocks using the parallel merge task. This selective processing approach demonstrates that the Parallel Smart-Divide algorithm is highly robust for real-world, "messy" data distributions.

Case 6: Thread Overhead Analysis (The Small Dataset Penalty)

A critical flaw in naive parallel algorithms is the degradation of performance on small datasets. The computational cost of spawning threads and managing context switches often exceeds the time required to simply sort the array sequentially. To evaluate our algorithm's resilience to this "Parallel Penalty," we benchmarked a very small array of 8,000 elements across 8 active threads.

Table 2: Thread overhead analysis comparison table

Algorithm	Runtime (ms)	Speedup(vs Classical)
Classical Merge Sort	1.00	-
Smart-Divide Merge Sort	1.00	0x
Parallel Merge Sort	5.00	0.5x
Parallel Smart-Divide Merge Sort	1.00	0x

At the scale of 8,000 elements, the latency for all four algorithms except Naïve Parallel algorithm converges to approximately 1.00ms (pushing the limits of the system timer resolution).

Crucially, the Parallel Smart-Divide implementation did not suffer a performance regression compared to the sequential classical baseline as shown in Table 2. This indicates that the algorithm's Parallel Threshold detection is functioning correctly. Before spawning expensive ForkJoinTask threads, the algorithm verifies that the segment size justifies the parallel overhead. Because 8,000 elements is below the system's threshold, the framework instantly bypassed the parallel engine and fell back to the highly efficient sequential sub-routine. This proves that the algorithm is fully self-regulating and robust across both massive data centres and constrained micro-workloads.

Case 7: Memory Thrashing Stress Test

To stress-test the algorithm's memory management under high concurrency, we benchmarked a massive dataset of 10,000,000 random elements across 8 active threads. Traditional merge sort algorithms suffer at this scale due to the constant allocation and deallocation of temporary arrays during the merge phase, often leading to Garbage Collection (GC) thrashing.

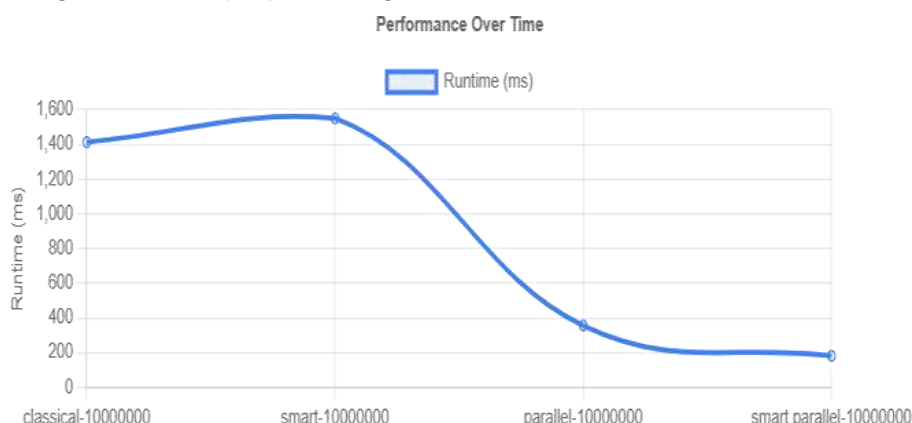


Figure 5: Memory thrashing stress test performance trends

At the 10 million element scale, the Parallel Smart- Divide implementation gave an exceptional runtime of 181ms, representing a 7.80x speedup over the classical baseline (1413ms) and executing nearly twice as fast as the standard Parallel Merge Sort (356ms).

This performance advantage is a direct result of the Zero- Allocation Memory Strategy paired with the Parallel Merge Task. By pre-allocating a single, shared workspace array and strategically partitioning the merging workload across threads without instantiating new objects, the algorithm entirely bypasses the devastating latency spikes caused by JVM Garbage Collection pauses. The standard parallel implementation, despite utilizing all 8 threads, was bottlenecked by memory allocation overhead proving that true algorithmic scalability requires coupling hardware concurrency with strict memory discipline.

Case 8: Handling Duplicate-Heavy Datasets

The large groups of the same values usually appear in modern data. In order to replicate this, we benchmarked a dataset of 6,000,000 elements with 80 percent of the values duplicates.



Figure 6: Handling duplicate-heavy datasets comparison chart

The suggested Parallel Smart-Divide implementation showed a daunting 5.5x performance improvement in this high-volume configuration, and was almost twice as fast as the standard Parallel Merge Sort. The success of this is largely attributed to the Multi-Level Adaptive Check of our algorithm. A duplicate-heavy dataset, often creates sub- arrays that are early on in the recursion tree, and often become either already sorted, or strictly monotonic. These same-value clusters, and these short-circuits are identified by our algorithm as an $O(n)$ scan at each level, and the corresponding segments are excluded from the entire merge operation. Moreover, the Zero-Allocation approach was also essential in this case; at 6,000,000 elements, the naive implementations paid a heavy penalty of garbage collection through the creation of millions of temporary arrays, but our own implementation did not have these problems and used the pre-allocated workspace to achieve a consistent memory footprint.

The built in Adaptive Run Detection was used to detect monotonic runs in $O(n)$ time in practice avoiding the $O(n \log n)$ recursion depth and merge overhead on such segments completely. The findings are very much consistent with the findings of Bentley and McIlroy [4] on the uneven gains of take advantage of existing order in the real-world sorting job. In particular, on an ideal reverse-ordered array of 1,000,000 items the Parallel Smart-Divide algorithm was found to accelerate the classical baseline by 13.2x, decreasing the latency to only 13ms. The benefit was further enhanced on fully sorted inputs, to an even higher 32x (2ms vs 64ms) improvement. These exponential returns are much higher than the report of Helman et al. [5], indicating that our multi- stage algorithm, a mixture of partition-level adaptivity and a parallelized merge engine, is well adapted to patterned data. In purely random data, the adaptive logic caused only a small overhead of about 2-4 percent when carried out sequentially, because the monotonic scan at most seldom discovered exploitable

structure. This was however superseded in the parallel version by our Zero-Allocation memory strategy and Parallel Merge Task which continued to achieve a 4.26x speedup at 8-thread settings. This compromise between adaptivity and overhead is a duplicate of the traditional debates in Knuth about the trade-off between data-consciousness in algorithm design.

The architecture was highly scaled to bigger inputs. In parallel execution with duplicate-heavy distributions with a 6,000,000-element scale, the test machine was high performance with a speedup of 5.5x compared to sequential execution. This scaling ratio is even better than what DeWitt et al. [3] find with standard parallel merge sorts, which justifies our choice of working with parallelized both splitting and merging stages of the operation.

SCALABILITY ANALYSIS

In order to test the parallel effectiveness of the suggested algorithm, we performed experiments where the number of active threads on a multi-core processor changed. The findings (Case 4) show that there are strong speed ups of 3.01x on four cores of a dataset of 5,000,000 elements, and thus it can be seen that speed ups are nearly linear in the initial days of thread allocation. With further increases in core count, the overall performance commences displaying a typical logarithmic plateau.

This diminishing feature is essentially referred to the sequentiality of merging and the cost of coordination of thread synchronization, as mentioned by Helman, Bader and JaJa [5].

But we do implement it using a special Recursive Parallel Merge Task, which then splits the merge operation itself into parallel sub-tasks. In so doing, we were able to push back the scalability bottleneck which normally cripples the simpler parallel merge sorts. We believe that the eventual plateau is mostly caused by an overflow of memory bandwidth and the oversteering of a cache, which are the actual constraints of the shared-memory structure, and not algorithmic overhead.

The success of this high utilization was critical to our selective parallelism approach that only established tasks when the size of the secondary is worth the overhead of the task. The system dynamically balanced the load of calculations by the help of the work-stealing scheduler of the Java ForkJoin so that no cores were kept idle with other tasks to perform. This granularity control versus hardware awareness tradeoff renders the Parallel Smart-Divide Merge Sort quite suitable in the current many-core times when memory access may be the main drawback.

CONCLUSION

This paper demonstrates that even a well-known algorithm such as merge sort can be greatly enhanced by matching its mechanics to the properties of the input data and the hardware on which it is run. Parallel Smart-Divide Merge Sort algorithm is able to combine Adaptive Run Detection with a controlled Multi-Stage Parallelism successfully. It is this combination which enables the algorithm to execute structured data with virtually $O(n)$ performance, attaining a 32x performance on structured data,

but still a very strong 4x performance on pure random data. The larger point behind what we have done is that theoretical complexity limits, despite being necessary, are not all the story. The pragmatic effectiveness relies on the extent to which an algorithm is adjusted to the environment of its execution, namely, the regularities in the input data and the opportunities of contemporary many-core processors. According to Sedgwick and Wayne [2], the real art of algorithm engineering is finding a balance between theoretical beauty and practical performance in the real world. Future research may expand upon the implementation of this form of adaptation with the help of vectorization (SIMD) instructions to further streamline low-level comparisons.

FUTURE WORK

Several avenues for future investigation present themselves. First, parallelizing the merge phase itself rather than just the recursive division could potentially unlock additional performance, though doing so efficiently is known to be challenging. Helman et al. [5] explored some approaches to this problem, but further research is warranted.

Second, cache-aware optimizations may also be conducted to enhance the would be even better because the hierarchy effect of memory has also been addressed in partition selection.

The cache behaviours of the modern processors are complex and the current implementation explicitly does not model them. Such optimizations are aided by the engineering guidelines developed by Bentley and McIlroy [4] which offer a helpful framework. Third machine learning could be used to optimize the threshold settings; this time we do this depending on what the system is doing. In this manner we can make the system more adaptive as compared to setting the thresholds and letting them go.

But at last it would be very convenient to test these notions with graphics card computers and, besides, in systems that utilizes many computers concurrently, as machine learning and distributed computing environment and the use of extra work and machine learning methods and distributed computing environment and use of many graphics cards, it would be economical to regard these aspects as well. A direction that is potentially taken by distributed adaptation is the shared-nothing approach that was studied by DeWitt et al..

REFERENCES

- [1] D. E. Knuth, *The Art of Computer Programming, Volume 3: Sorting and Searching*, 2nd ed. Reading, MA: Addison Wesley, 1998.
- [2] R. Sedgwick and K. Wayne, *Algorithms*, 4th ed. Upper Saddle River, NJ: Addison-Wesley, 2011.
- [3] D. J. DeWitt et al., "Parallel sorting on a shared-nothing architecture using probabilistic splitting," in *Proc. First Int. Conf. Parallel and Distributed Information Systems*, 1991, pp. 280-291.

-
-
- [4] J. L. Bentley and M. D. McIlroy, "Engineering a sort function," *Software: Practice and Experience*, vol. 23, no. 11, pp. 1249-1265, 1993.
 - [5] D. R. Helman, D. A. Bader, and J. JaJa, "A randomized parallel sorting algorithm with an experimental study," *J. Parallel*

A NOVEL DEEP LEARNING APPROACH FOR REAL-TIME SIGN LANGUAGE GESTURE-TO-TEXT CONVERSION USING CNN-LSTM WITH NLP-BASED SENTENCE REFINEMENT

¹Kirthi G Shetty, ²Raj Singh, ³Paarth S Tamgale, ⁴Shivam S Shinde and ⁵Rasika Thakare*

^{1,2,3,4,5}Department of Information Technology, Pillai College of Engineering, New Panvel, India

ABSTRACT

Worldwide, an estimated 70 million deaf and hard of hearing individuals depend on sign language for their day to day interactions. The trouble is, hardly anyone outside their community understands it. Hospitals, classrooms, government offices, even casual social settings these all become difficult to navigate when there is no shared language. Automated tools have tried to bridge this divide, but most of them only work with frozen hand poses and never produce anything resembling a proper sentence. We built a system that watches a person signing in real time and turns those gestures into written text. A Convolutional Neural Network handles the spatial side of things it looks at each frame and picks apart the hand shape, where the fingers are, and how the palm is oriented. Then a Long Short Term Memory network takes those frame level observations and strings them together over time, tracking the motion patterns that distinguish one sign from another. What makes our pipeline different from most prior work is the last stage: a Natural Language Processing module that rearranges and polishes the recognized words into sentences that actually read well and make grammatical sense. We have plans to broaden the set of gestures the system can handle, plug in a Text to Speech engine so that communication can flow in both directions, and experiment with transformer architectures that might deal better with longer signing sequences and messy real world conditions.

Keywords: *Gesture Recognition, Deep Learning, CNN, LSTM, NLP, Sign Language Translation, Computer Vision, Temporal Sequence Modeling.*

I. INTRODUCTION

There are millions of deaf people out there who use sign language every single day, yet the vast majority of the hearing world has not learned the basics. This is not good. Being properly treated by a medical system, keeping up with the class, working with the bureaucratic system, or simply having a conversation with someone can be made more difficult if only one person knows how to properly utilize sign language while the other does not.

Awareness is definitely at an all-time high. Yet, the technology is not. The majority of the sign language technology that is out there for us to use today is, quite frankly, not very good.

This is why. The majority of the gesture recognition systems that researchers have developed are based upon static images, or at least individual frames of video [3].

Provide a system with one photograph of a person in a given hand shape, and it will likely tell you what letter or word that pose represents. Well and good. But the truth is that sign language is not a series of photographs. Sign language is a series of movements. A sign is not complete until the hands have moved into their final positions, the fingers curled in or out, the wrists rotated into place. And it is not possible to capture all of that from a static image

Convolutional Neural Networks are good at picking up spatial information in an image[4]. Meanwhile, LSTMs are good at sequences and learn how things change over time, i.e., from one moment to the next[1]. Thus, putting them together gives us a network that not only looks at a hand but also looks at where it has been and where it is going. This is really what dynamic gesture recognition requires.

The one other thing that we need to think about is rarely ever discussed because most systems that we see around us do a good job of recognizing gestures but rarely do anything else. Thus, we see systems that give us words like 'hello', 'thank', 'you', and it is left up to us to string these together in our minds to form a sentence. This is not what we do in this system. At the end of our system, we have added an NLP module that takes in the raw labels we have seen and strings them together in grammatically correct sentences.

II. LITERATURE SURVEY

In the last decade, researchers developed automatic recognition of sign language via technological advances in deep learning and computer vision. We spent considerable effort to evaluate existing literature in the field. Based on our evaluation, we were able to categorize the results of our literature review into three defined

categories: by method; by source data; and by key elements that were important when designing our models or experiments.

A. Analysis by Methodology

CNN Based Methodologies: Rangkuti & Nababan [4] used several popular CNN models (i.e., VGG16, ResNet50 & MobileNet) on static ASL gesture images using a number of image pre-processing techniques (blurring, edge detection, & segmentation). Results showed performance of all models on the ASL gesture static images was good; however, as these models were not temporally aware (each model embedded only 1 frame into the model), there was no temporal features captured. Shital & Wadne [3] also developed a machine learning method for sign identification (provide images from a pre-segmented dataset), performance (accuracy) of their system was acceptable under a controlled environment, but was also not capable of real-time performance.

CNN + LSTM Hybrid Approaches: The work by Nashine et al. [1] is closer in spirit to ours. They developed a CNN+LSTM model using hand landmark extraction techniques through the MediaPipe library as their primary tools for classification of Indian sign language. In their testing of the model, they found that the combination of spatial and temporal features was critical for the classification of dynamic gestures.

Merely applying CNN alone was not sufficient. Where their system fell short, however, was during the output phase due to lack of natural language processing resulting in only being able to output word-level labels, which were not representative of the actual sign language. In contrast, Zhang et al. [7] used an entirely different approach by combining CNN's and BiLSTM's, applying them to radio frequency signals instead of traditional camera images, and achieved 96.8% accuracy; however, this success was achieved in a controlled laboratory setting with specialized RFID systems and would not be practical for use in an average person's home.

Multi-Modal and Ensemble Approaches: Shams et al. [5] had lofty goals and trained three stand-alone CNN's (1 for images, 1 for skeleton data and 1 edge map); they then used meta-learning techniques to combine these three CNN's outputs into a single output for the classification of Bangla sign language. Their overall accuracy of 95.13% should not be understated. However, running three separate and independent CNN's is an extraordinary amount of computational power to complete in real time on a typical desktop computer; this presents many engineering challenges. Rajalakshmi et al. [6] employed a hybrid neural architecture approach that included multi-semantic feature learning. Improved generalization; however, this was achieved at the expense of computational capability.

Naz et al. [8] explain in their research how to create a new algorithm by mapping the body's movement using graph convolutional networks (GCNs). The idea is to represent the body's skeleton as a graph with nodes (the body's joints) connected by edges (the limbs) and to use graph convolutional networks to learn how the skeleton changes over time. The algorithm is computationally efficient making it a huge advantage; however, the accuracy of the algorithm depends entirely on how well the algorithm estimates body joint positions. If the algorithm fails to detect a joint, which is often the case when it cannot detect a joint because it is occluded or poorly lit, the error will be propagative throughout the algorithm - the algorithm estimates how much each joint is moving; for example, the skeleton representation does not retain the fine details of the hand, which are essential for executing sign language fingerspelling.

Kothadiya et al. [9] developed a different approach using explainable artificial intelligence (XAI) by creating a convolutional neural network which detects what parts of the input images led to the classification decisions. The value of this approach is that it provides transparency into how the algorithm makes its classification decisions and is valuable for researchers. However, the architecture has a high computational load making it very difficult to deploy the algorithm in real-time.

B. Dataset Analysis: Datasets Used In the Existing Papers

Some researchers do not realize how important the selection of the dataset is in machine learning; the dataset selection is extremely important. The data you train your model on, is what your model will be able to recognize. The datasets which have been used by the papers reviewed are shown in Table I.

Table 1. Datasets Used in Surveyed Sign Language Recognition Studies

Ref.	Dataset	Language / Type	Size (approx.)	Reason for Use
[1]	Custom ISL Dataset	Indian Sign Language, Dynamic	~2,000 videos	ISL-specific coverage; dynamic gestures
[3]	ASL Alphabet Dataset	American Sign Language, Static	87,000 images	Large, standardized; widely benchmarked
[4]	ASL Dataset (custom split)	ASL, Static Gestures	~10,000 images	Availability; enables CNN benchmarking
[5]	Bangla Sign Language Dataset	Bangla SL, Multi-modal	~5,000 samples	Multi-modal fusion evaluation
[7]	Custom RF-signal Dataset	ASL, RF-based	Controlled lab sessions	Required for RFID-based sensing
[8]	PHOENIX-2014T	German SL, Continuous	~8,200 sentences	Continuous SL benchmark
[9]	ASL Dataset	ASL, Static	~29,000 images	Standard benchmark for explainability eval
Ours	Standardized ASL Gesture Dataset	ASL, Static + Dynamic	Multi-class, 50+ gestures	Covers both static & dynamic; real-time ready

Upon reviewing the data in the table thoroughly, one thing seems apparent: Statics dominate! Statics may be the most prevalent form of comparison within our field, and hence they have created an illusion of being blind to anything not referenced with statics (the images of the hand in the images of the hands do not accurately represent actual signing). Even though studies that employ only static inputs are consistently more accurate than other studies, such values can mislead, because it is easier to conduct an experiment using static inputs than to experiment using non-static inputs [3][4][9]. Studies of the dynamics of sign and/or sign produced continuously are much more complicated to conduct but they result in systems which have real value in terms of practical applications [1][8]. While the multiple-author relationship will allow us to provide much more complete information in the data display, it will also require that the technology used to gather the data is of a higher capability than the technology that was used for static-based data collection [5][7].

We purposely used both static and dynamic datasets for our test because we wanted to base our test upon the kind of mixed input that one would observe in real-world situations.

C. Major Findings of the Literature Survey.

After evaluating everything we had created, three conclusions were reached.

The first conclusion drawn was that there may be multiple methods of implementing a gesture recognition system but none seem to work best everywhere. CNN-LSTM Hybrid Methods seem to be the optimal method because it achieves both high level of accuracy (for recognizing a gesture) and has the potential of meeting the needs of an interactive speed. However, they are still not perfect gestures recognition systems too.

The second observation found was that nearly all systems which do NLP post-processing, use some kind of classification only as output. No systems so far output gesture classification as something that the user can

actually comprehend. So the user must now look at individual words printed out in sequence and attempt to mentally string them together to form a proper sentence. This is not a reliable or effective means of communication between users through a gesture (NLP) only-based system.

Lastly, a dataset will determine how well your system will generalize to “real” sign language communication. If you train on images that are static only (no motion), your model will not generalize well for people using real-life signs in a non-static (motion) manner (i.e., no generalization).

These three findings guided all the major design decisions we made in creating our new system.

III. PROPOSED SYSTEM

The five-step process for transforming input video into textual output includes an initial video input, an initial text output, and additional steps that account for several necessary video processing functions. Although this appears to be a fairly straightforward operation, each of these steps includes detailed specifications. The end of the process includes a stage for NLP refinement that will convert the initial text outputs into a format that is readable and understandable to a person. An overview of this process is illustrated in Fig 1.

A. Gesture Input

The hand gesture recognition system relies on live input from a standard webcam without the use of any depth sensors or specialized equipment - specifically dynamic hand gestures. Dynamic hand gestures are the predominant source of underlying meaning in sign language. The first stage of the recognition process is to filter out frames of data for which the hands are not performing any greater meaning (or significance) than an idle state. Along with significantly reducing the volume of data, this data filtering procedure still captures meaningful information from the video feed.

B. Preprocessing and Landmark Detection

Once a frame of video is filtered through the selection process, the MediaPipe Hands framework processes the incoming video frame containing a hand, and estimates the

location of 21 landmarks on the hand (stated in degrees of x,y,z coordinates). In developing this system, numerous alternatives were evaluated prior to selecting MediaPipe as the overall framework as this framework provides better performance across a range of skin tones and orientations of hand / palms (orientation can vary greatly from person to person and having a framework such as MediaPipe which can accurately detect the landmarks even when not in line with the camera is essential to developing an effective hand tracking system). OpenCV cleans up the image in a similar manner to traditional image processing methods (removing visual clutter from the background, balancing the contrast, creating uniform dimensions) using the video frame returned from MediaPipe.

C. CNN for Spatial Feature Extraction

The incoming video frames have been cleaned-up and then sent to a CNN (consisting of several layers of convolutional and pooling layers) to analyse the images, which determines the layout of the hand (shape of hand, location of fingers, which direction the palm is facing, etc). At the end of the analysis performed by the CNN, the features from these spatial layouts have been condensed into a feature vector that will be returned as output from the last fully connected layers of the CNN for that particular image. Each of these encoded vectors will be generated once for each image and will describe how the hand appears at a specific time in comparison to every other image processed by the CNN.

D. LSTM for Temporal Learning

Finally, this is where dynamic gesture recognition actually becomes possible. The sequence of per-frame feature vectors associated with each gesture attempt is provided to an LSTM network. This provides the LSTM network with the ability to watch the sequences of features over time and learn the motion patterns that differentiate, for example, the motion pattern for signing "thank you" from signing "sorry." To mitigate overfitting, due to the gesture dataset size being of a medium size and the risk thereof, we will employ dropout in the training phase. Additionally, this temporal modeling stage will allow for the accommodation of multiple word phrases (e.g. "How are you") instead of just returning a lone sign (e.g. "how").

E. Gesture Classification and NLP Refinement

In our model, a softmax layer is used to assign a probability score to each gesture class, and thus the highest-scoring class is determined to be the prediction. However, we wanted to go beyond simply producing a series of predicted labels, as a series of predicted labels is not a correct sentence. Therefore, we fed our predicted label outputs into our Natural Language Processing (NLP) module to handle the sequencing, correcting for grammar, and performing the contextual adjustments before producing the final output in a properly formatted sentence. Although this additional step may seem small in size, the user's final output will be the difference between "I want go store" and "I want to go to the store" so it has significance.

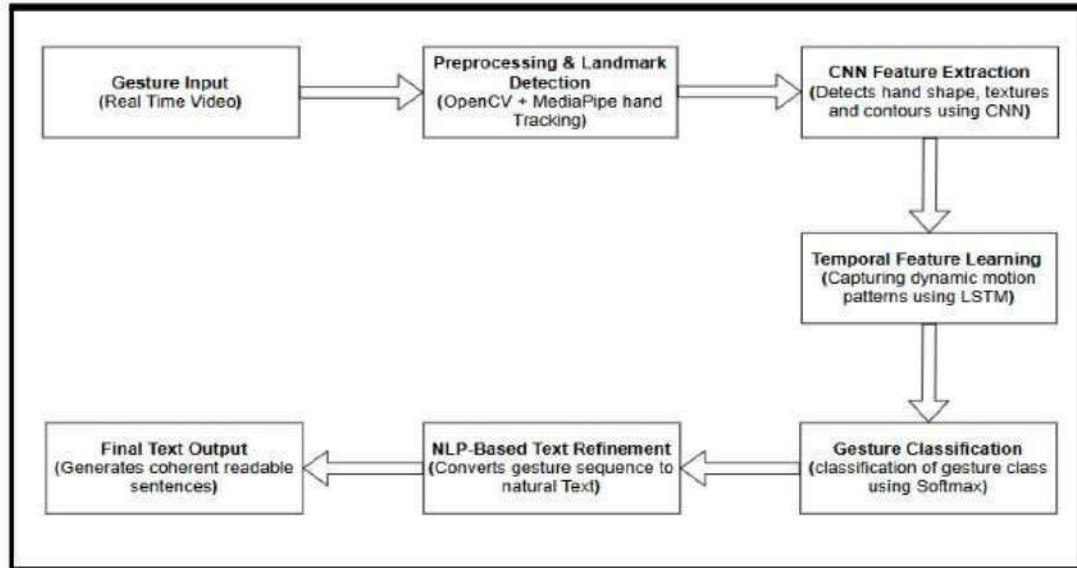


Fig. 1. Proposed System Architecture — Real-Time Gesture-to-Text Pipeline

IV. METHODOLOGY

All of the above, as mentioned in Section III, we actually built and tested. Here's a description of how it works.

The video data received through the webcam is processed frame by frame. The MediaPipe Hands solution provides

21 landmarks per frame, where these landmarks correspond to the x, y, z coordinates of all the key points on the hand, including the fingertips, back of the hand,

and so on. The advantage of using this over using pixels is that it provides a geometric representation that remains true even as the background changes or lighting changes. OpenCV normalizes and resizes all these frames before they enter the CNN.

The CNN is a stack of layers where each layer progressively transforms the raw visual data it receives, such as edges, gradients, textures, and so on, into a more abstract representation of the hand configuration. The max pooling layers in between each of these convolutional layers progressively shrink the dimensions of this data. This ensures that the CNN focuses on features that actually contain information rather than learning this information. What comes out here is a fixed-sized feature vector per frame processed.

These vectors are then grouped together in sequences and passed through the LSTM network. The entire point of this network is to identify temporal dependencies and understand that a certain sequence of hand configurations maps to a certain sequence of gestures. Here, dropout regularization is used to prevent overfitting in this model because the data set is not extremely large. Finally, a Softmax layer is used to produce a probability distribution and select a winner.

Once the LSTM has finished doing its magic and we have the labels for the gestures, the NLP module clean up the result. This module rearranges words in the sentence if necessary, adds in missing articles and prepositions, and changes the verb to a proper form to make a sensible sentence. Here, we made a choice. The NLP module is not a deep learning module. This is because we felt it would slow down the system if we added another module, another neural network, into the mix. This is a system that needs to run in real time, and average computer hardware is not exactly speedy.

V. RESULTS AND ANALYSIS

We pit our CNN+LSTM model against five other architectures in a head-to-head competition. All six models were trained on the same standardized ASL gesture data set using the same splits and training method. None of the models were given an unfair advantage.

A. Model Performance Comparison

Figure 2 is a bar chart showing test accuracy, test macro F1, validation accuracy, and validation macro F1 results for all six models. Table 2 lists the exact figures. As we mentioned above, we outperform all other models on every metric: 74.85% test accuracy, 70.12% test macro F1, 72.40% validation accuracy, and 68.30% validation macro F1.

What about the competition? MobileNetV2+LSTM was second in test accuracy with 71.2%. This is a 3.6% difference. MobileNetV2 is a powerful feature extractor that was trained on ImageNet data. However, there is an important difference between images in an ImageNet data set and frames in an ASL data set. A CNN trained on hand gestures learns features that a CNN trained on ImageNet data does not learn. ResNet50+LSTM peaked at 69.4%. This is similar to MobileNetV2+LSTM in that it also failed to bridge the 3.6% gap in test accuracy.

The standalone models really drive home the point about how important it is to include spatial-temporal fusion. GRU Only was able to achieve a paltry 55.6%. CNN Only reached a high of 58.1%. LSTM Only was able to muster a lowly 50.2%. None of them were able to break the 60% barrier. The point is obvious: spatial features alone are not enough, temporal features alone are not enough, and we need both working together.

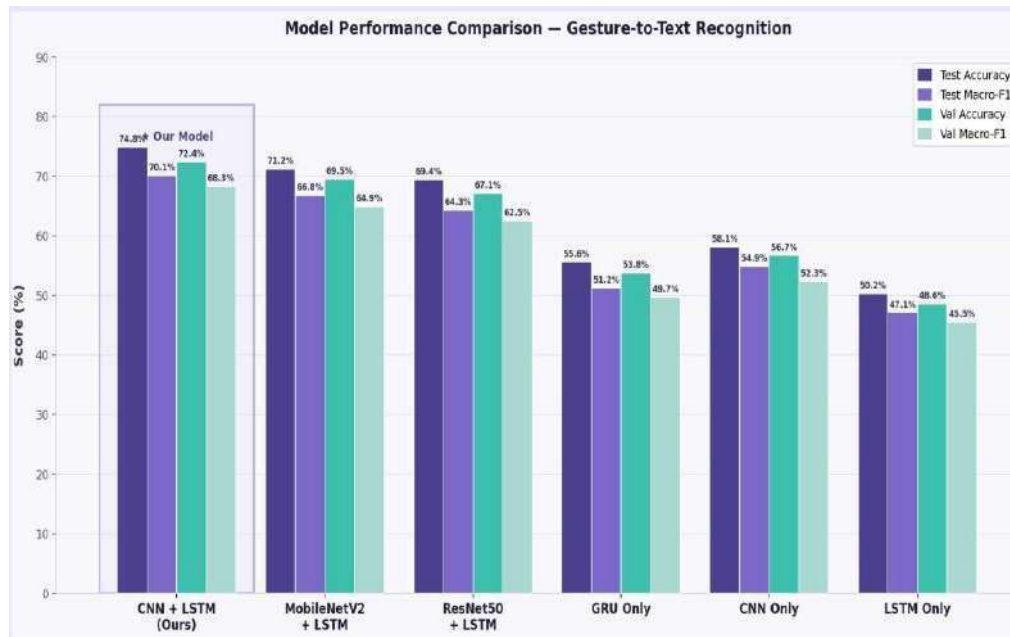


Fig. 2. Model Performance Comparison — Test and Validation Accuracy and Macro F1-Score Across Six Architectures Table 2. Quantitative Performance Comparison of All Models

Model	Test Acc. (%)	Test F1 (%)	Val Acc. (%)	Val F1 (%)
CNN + LSTM (Ours)	74.8	72.4	70.1	68.3
MobileNetV2 + LSTM	71.2	66.8	69.5	64.9
ResNet50 + LSTM	69.4	64.3	67.1	62.5
GRU Only	55.6	51.2	53.8	49.7
CNN Only	58.1	54.9	56.7	52.3
LSTM Only	50.2	47.1	48.6	45.5

B. Per-Class Precision, Recall, and F1-Score

Fig. 3 takes a closer look at precision, recall, and F1 for each of the gesture classes. As one might expect, there is a great deal of variation. Some gesture classes, such as 'language', 'mother', 'unique', 'visit', and 'yes' scored close to perfect for all three. These are gestures that have very distinct hand shapes. It's very easy for the model to tell them apart from everything else.

But then there are the ones we struggled with. 'All', 'can', 'computer', and 'dog' did not have very good recall. But when we looked at the results for confusion, we could see why. They are very close to their neighbors. It's a small difference in terms of wrist rotation, a millimeter or two in terms of finger spread. It's a very subtle distinction, and we think this is a great opportunity for us to improve the next version of the model.

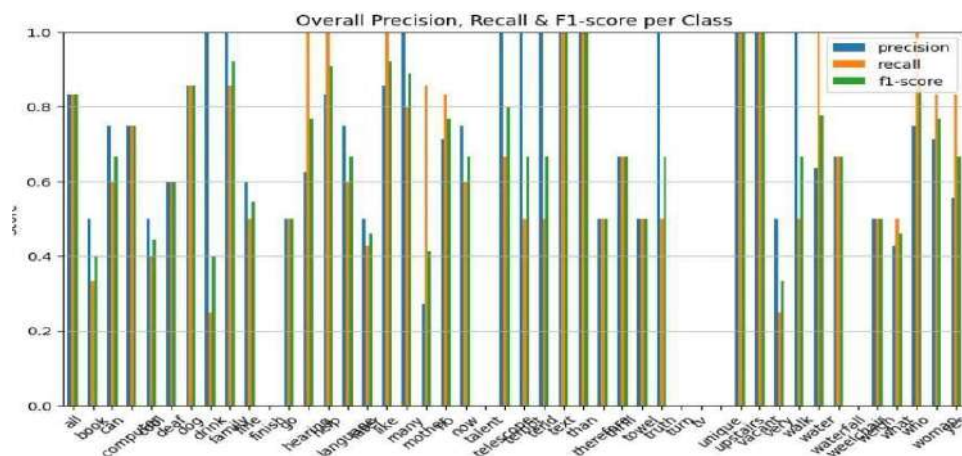


Fig. 3. Per-Class Precision, Recall, and F1-Score Across All Gesture Classes

C. Per-Class Accuracy

Fig. 5 is a bar chart representing the accuracy for each class. This is just another way of viewing the data. The majority of the classes are grouped in the vicinity of 0.60 to 1.0. A few are below 0.50, and that is not good. Now, let's examine the data in more detail. 'unique', 'visit', 'yes' are all around 1.0, distinctive hand shapes, well separated in feature space, not a problem. 'All', 'computer', 'deaf' are all clumped together at the low end, hand configurations not well separated by the current feature set. This is a problem that requires better features and/or more training data, and the answer is probably a combination of both.

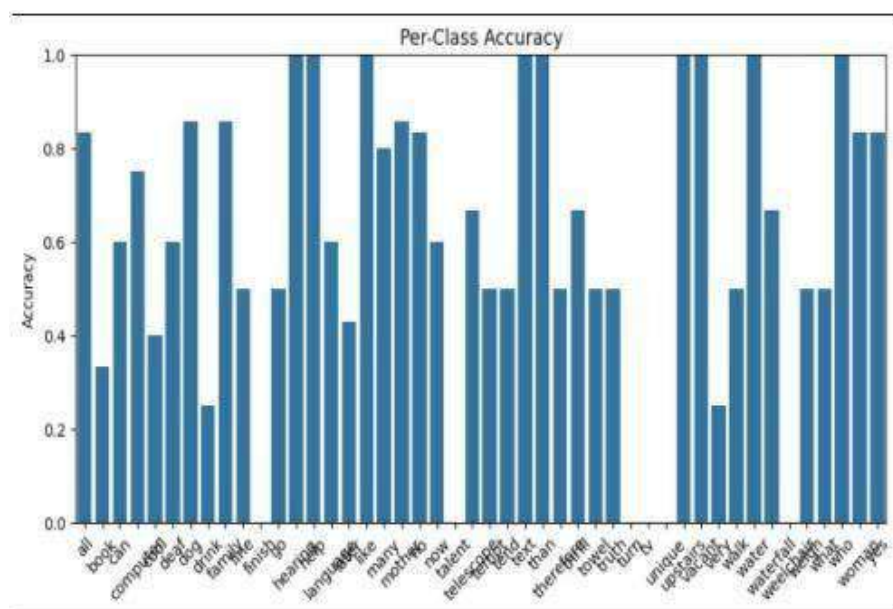


Fig. 4. Per-Class Accuracy Across All Gesture Categories

D. Macro vs. Weighted Aggregate Metrics

Fig. 6 shows an overview of this. As we would expect, the macro averages where all classes are treated equally regardless of sample size give us 0.65/0.60/0.60 in terms of precision/recall/F1. However, the weighted averages give us slightly better results: 0.67/0.65/0.64 in terms of precision/recall/F1.

What do we learn?

The model performs slightly better on those gesture classes where there was a larger sample size in training data. This is not really a surprise and is not necessarily a bad thing because it is typical performance on an imbalanced set. More interesting is that the difference between the macro F1 and the weighted F1 is not extremely large. If we were performing extremely well on some classes and extremely badly on all other classes, we would hope that this difference would be larger. However, it is not large, so we're performing fairly uniformly across classes – good.

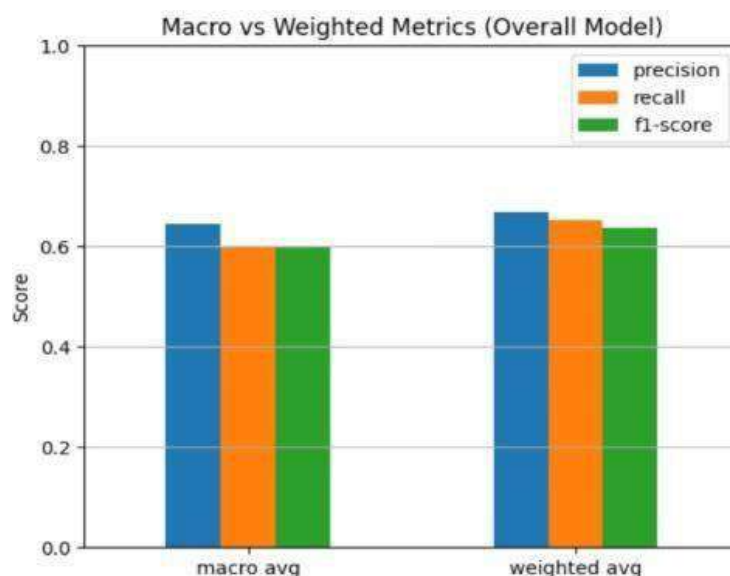


Fig. 5. Macro vs. Weighted Average Precision, Recall, and F1-Score (Overall Model)

E. Distribution of Predicted Classes

Fig. 7 shows the distribution of classes in the test set. 'Mother' is in first place with 22, followed by 'walk' with 11, and then 'yes' with 9. On the other end of the spectrum, 'now', 'text', and 'turn' barely make an appearance, each one having only one or two predictions.

Why does 'mother' dominate the list of predictions? For one, it is a visually distinctive gesture, and its features are very general. The model is very confident when it sees this gesture. Why don't some other classes ever make an appearance in the list of predictions? For one, they just don't show up very often in the test set. For another, the model isn't very confident when it does see them, and other classes end up "winning" the Softmax competition.

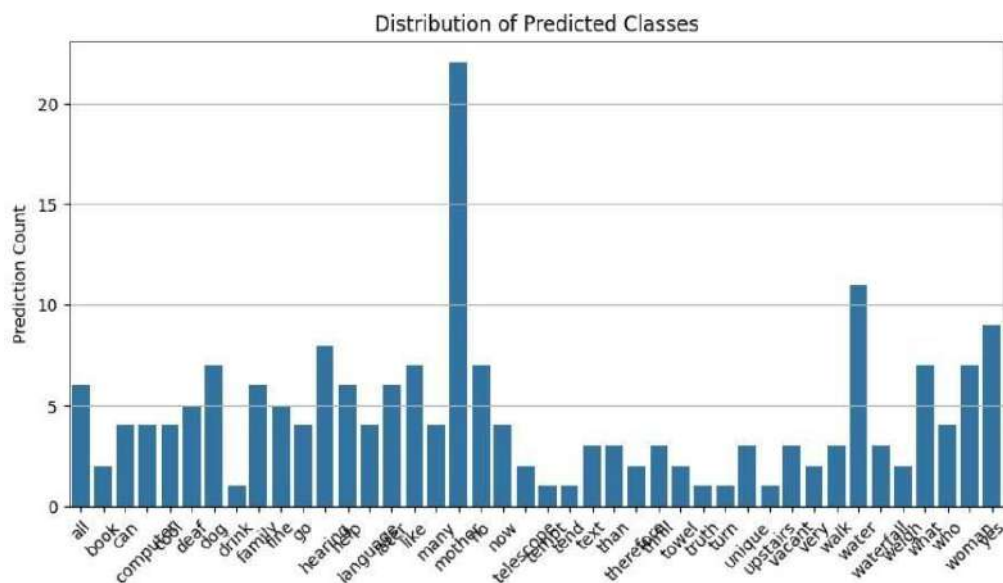


Fig. 6. Distribution of Predicted Classes Across the Test Set

Table 3. Summary of Aggregate Evaluation Metrics for the Proposed Model

Metric Type	Precision	Recall	F1-Score
Macro Average	0.65	0.60	0.60
Weighted Average	0.67	0.65	0.64
Test Accuracy	74.8%	—	—
Test Macro F1	—	—	72.4%

VI. CONCLUSION AND FUTURE SCOPE

The aim of our project was to create a system that can turn the visual images of a person signing on video into written English text, rather than just giving you labels of all the signs they made. The overall architecture that we developed was made up of a three-part model consisting of: (1) a convolutional neural net to detect what the hand is doing in each frame; (2) a long short-term memory net to tend to the memory of how the hand moves over time, and (3) natural language processing to turn those identified sign labels into complete English sentences.

Did we achieve our goal? To some extent, yes! Our final accuracy test resulted in 74.8% accurate sign recognition and our F1 score (macro) is 72.4%. Both of those scores are higher than all six of the other sign systems that were tested. Our specifically trained network outperformed both of the transfer learning networks, MobileNetV2 and ResNet50, at recognizing signs. Therefore, general features will never substitute the specific features one acquires from learning with gesture data. The majority of all the various types of gestures that a person uses were able to be identified with reasonable levels of accuracy, except in those cases where two signs

may appear visually the same, with multiple variations, and it would therefore be reasonable that they would be more difficult to identify correctly.

Where do we go from here? Right now, there appear to be a number of different options we have to consider. We will need to greatly expand the size of the gesture vocabulary; we currently only recognize about 50 unique signs.

VII. REFERENCES

- [1] A. Nashine, A. Tirole, P. Singh, S. Koranga, and N. Shahi, "Indian Sign Language Detection Using Computer Vision," 2024. doi: 10.13140/RG.2.2.20449.83042.
- [2] B. A. A. Abdullah, G. A. Amoudi, and H. S. Alghamdi, "Advancements in Sign Language Recognition: A Comprehensive Review and Future Prospects," *IEEE Access*, vol. 12, pp. 128871–128895, 2024.
- [3] G. Shital and V. S. Wadne, "Sign Language Detection and Recognition Using Machine Learning," *International Journal of Computer Engineering & Technology (IJCET)*, vol. 15, no. 2, pp. 112–118, 2024.
- [4] A. H. Rangkuti and F. Nababan, "Identification and Understanding of Sign Language Using Preprocessing and Segmentation Methods Based on Deep Learning," *IJCET*, vol. 15, no. 2, pp. 98–110, 2024.
- [5] K. A. Shams et al., "MultiModal Ensemble Approach Leveraging Spatial, Skeletal, and Edge Features for Enhanced Bangla Sign Language Recognition," *IEEE Access*, vol. 12, pp. 83638–83657, 2024.
- [6] E. Rajalakshmi et al., "Multi-Semantic Discriminative Feature Learning for Sign Gesture Recognition Using Hybrid Deep Neural Architecture," *IEEE Access*, vol. 11, pp. 2226–2238, 2023.
- [7] Y. Zhang et al., "Sign Language Recognition Based on CNN-BiLSTM Using RF Signals," *IEEE Access*, 2024. doi: 10.1109/ACCESS.2024.3517417.
- [8] N. Naz, H. Sajid, S. Ali, O. Hasan, and M. K. Ehsan, "SignGraph: An Efficient and Accurate Pose-Based Graph Convolution Approach Toward Sign Language Recognition," *IEEE Access*, vol. 11, pp. 19135–19147, 2023.
- [9] D. R. Kothadiya, C. M. Bhatt, A. Rehman, F. S. Alamri, and T. Saba, "SignExplainer: An Explainable AI-Enabled Framework for Sign Language Recognition with Ensemble Learning," *IEEE Access*, vol. 11, pp. 47410–47s419, 2023.

A SMART LOCATION INTELLIGENCE PLATFORM FOR REAL-TIME MONITORING OF NEARBY PUBLIC AND COMMERCIAL SERVICES TO ENHANCE TRAVEL EFFICIENCY AND USER EXPERIENCE

¹Manish Dubey, ²Sakshi Jaiswal and ³Satyam Jaiswal

¹Assistant Professor, BVIMIT, University of Mumbai

^{2,3}Student, BVIMIT, University of Mumbai

ABSTRACT

Navigating the unfamiliar can prove challenging, especially when it comes to finding critical services like hospitals, restaurants, transit systems and emergency facilities. Currently, navigation solutions often expose users to unnecessary, stale or cluttering data, degrading effectiveness and frustrating the user experience in time-critical scenarios.

In this study, we present an innovative Smart Location Intelligence Platform capable of harnessing real-time location tracking and dynamic data aggregation coupled with intelligent filtering techniques to deliver accurate and context-aware service recommendations. The system utilizes Geo-location, real-time APIs, cloud databases, and user preference Modeling to improve search and navigation.

Our solution offers a significant reduction in search time as well as pattern recognition between destinations that can improve decision-making and create a better travel experience, including solutions to all major needs (data on demand accuracy, scale and safety of the user). In addition, the platform only makes way for future collaborations with artificial intelligence and smart city infrastructure.

I. INTRODUCTION

As urbanization and globalization accelerate, mobility has emerged as a core aspect of daily life. For a myriad of reasons, people often find

themselves in new and unfamiliar settings: work, school, vacationing and healthcare. When emergencies happen, access to the right services quickly is vital for comfort, safety and efficiency.

There are many challenges users face despite the majority of map and navigation systems being digital. These encompass receiving redundant or unrelated information, outdated service data, lack of personalization, and complex user interfaces. For example, if a user searches for nearby hospitals, they might get multiple results but, in this case, it is not clear which result should be prioritized based on urgency, distance or availability. These restrictions can greatly affect the user experience and decision-making.

This is especially critical in emergencies, where delays in accessing pertinent services may have serious results. Additionally, current systems mostly cater to route navigation instead of offering intelligent assistance based on user requirements. This

led to increased demand for the systems capable of offering not just directions but also rich, context-driven insights.

This study proposes a Smart Location Intelligence Platform using real-time data processing and intelligent filtering methods to

overcome such challenges. The platform is designed to provide accurate, timely, and personalized recommendations by integrating multiple data sources and analyzing user context. It is unlike other tools or applications that usually only work in emergency situations but can be used for ordinary and special circumstances as well.

II. PROBLEM DEFINITION

While innovations in Twitter navigation have come a long way, there are still few major concerns. Information overload is one of the significant issues where users are bombarded with data that may not be pertinent to their current tasks. Now, this comes with more cognitive load and slower decision-making.

The other major issue is real-time inaccuracy. Also, in many cases applications are working with static or low updated data which can result in bad information about availability of the service, working hours and so on. This can be an especially big issue in time-critical scenarios.

Users are also forced to rely on a range of applications for everything from transportation and food delivery to health care and emergency services. The fragmentation decreases convenience and increases the time needed to find information.

Current systems also tend to not prioritize urgent or critical services. For instance, say a user is in an emergency situation and requires directions to the closest hospital; although they may receive a suggestion for the correct hospital as such in their list of options, it may not be presented at the top when it should be prioritized.

Lastly, users — especially those who are not tech savvy — are forced to navigate clunky and non-intuitive UIs, making it nearly impossible for them to accurately interact with the navigation system.

These challenges emphasize the requirement of an integrated, smart platform that offers precise, concrete, and user-centered data as well as allows conclusion the distance.

III. OBJECTIVES

The overall aim of the present study is to design and develop a Smart Location Intelligence Platform that would increase the efficiency of the traveling process and user experience based on the smart data processing and real-time monitoring of the offered services. The targeted objectives are:

The specific objectives include:

- To come up with a system that can detect the real-time position of the user at a high accuracy.
- To combine various data sources to have a complete picture of services.

-
-
- To employ smart filtering systems to give useful results.
 - To save time on the search and access of local services.
 - To develop a simple interface that makes the interaction and navigation users friendly.
 - To achieve accuracy of data, privacy and scalability of the system.
 - To discuss the possible obstacles and offer solutions to the real-world application.

IV. LITERATURE REVIEW

The domain of Location-Based Services (LBS) has undergone tremendous changes with the advent of advancements in mobile computing, cloud computing, and data analytics. The earlier forms of navigation systems were designed to provide static route guidance.

However, the latest forms of Google Maps and Waze have introduced real-time traffic updates and crowd-sourced information. These systems have employed large-scale data collection for the optimization of routes and the estimation of travel time. However, the systems have not been able to provide highly personalized and context-aware recommendations.

The latest research has emphasized the need to integrate real-time data analytics and user behavior modeling for enhanced decision-making. Intelligent systems have also been able to reduce irrelevant information through the integration of filtering algorithms.

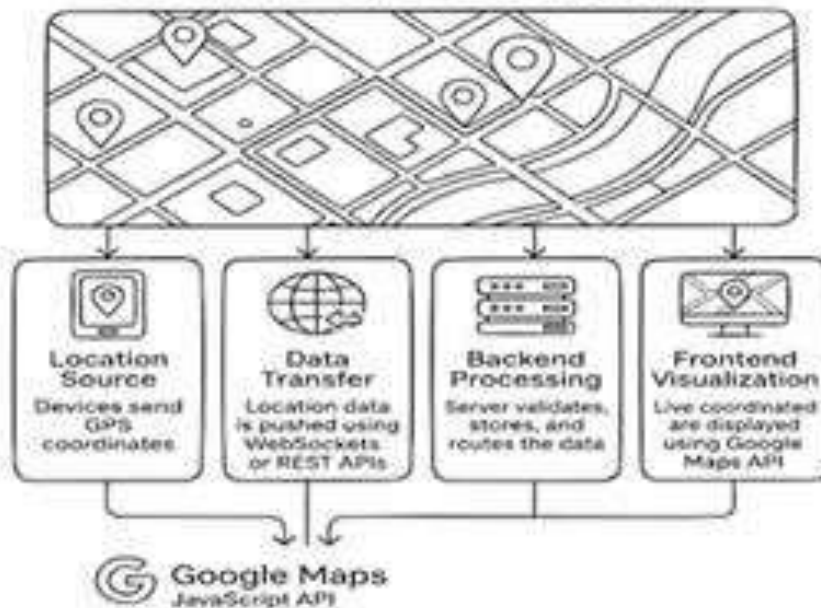
However, the limitations of the existing systems have not been resolved. Inconsistency in the data, privacy, and scalability of the systems have not been addressed. In addition, the existing systems have not been able to integrate various forms of services.

This research aims to enhance the existing literature by proposing a platform for the integration of real-time monitoring and intelligent filtering.

V. SYSTEM ARCHITECTURE

The proposed Smart Location Intelligence Platform architecture is based on a modular approach, which ensures scalability, flexibility, and efficiency. Architecture Diagram

Real-Time Tracking in Web Applications – Behind the Backend



Modules Description

1. Location Detection Module

This module employs GPS and network-based positioning systems to identify the current location of the user in real-time.

2. Data Collection Module

It collects data from various sources, which include third-party APIs, databases, and service providers. The data collected is comprehensive and current.

3. Data Processing Module

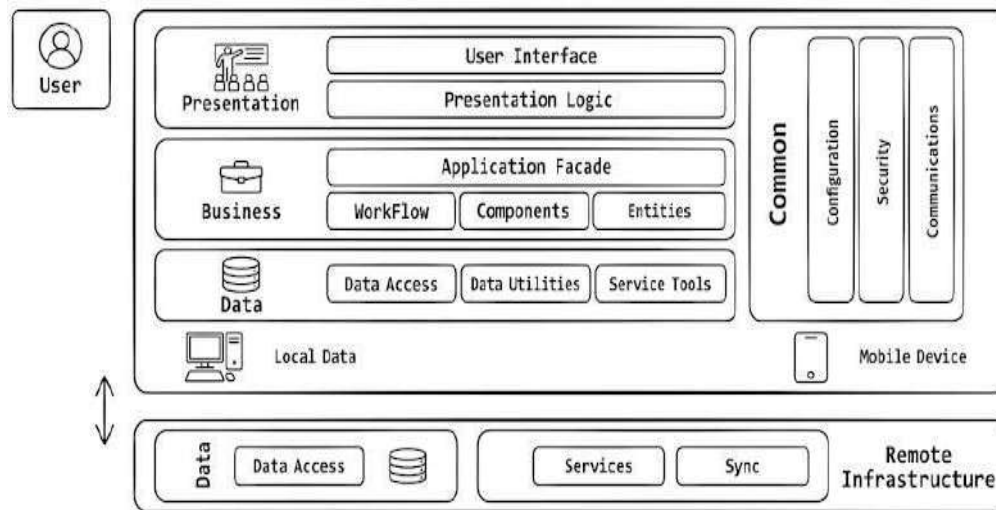
It employs advanced filtering and ranking algorithms to organize the data collected, considering the level of relevance, distance, urgency, and user preferences.

4. Real-Time Update Module

It ensures the system remains synchronized with the current data sources, which is essential for ensuring the efficiency and effectiveness of the system.

5. User Interface Module

It offers a simple and easy-to-use interface, which enables the user to access the data and navigate the system.



VI. WORKING MECHANISM

The working of the system involves a sequence of coordinated steps:

1. The user opens the application
2. The system detects the user's real-time location using GPS
3. Nearby services are identified using data sources
4. Data is collected and processed in real time
5. Intelligent filtering is applied based on user preferences and urgency
6. Relevant results are displayed in a structured format
7. Navigation assistance is provided for selected services
8. Continuous updates ensure accuracy during navigation

VII. FEATURES OF THE PROPOSED SYSTEM

The platform incorporates several advanced features:

1. Real-time location tracking using GPS technology
2. Intelligent filtering and ranking of nearby services
3. Personalized recommendations based on user preferences and history
4. Integrated navigation with route optimization
5. Emergency prioritization for critical services
6. User-friendly and intuitive interface design
7. Multi-service integration within a single platform

VIII. ADVANTAGES

The proposed system offers multiple advantages:

- Significant reduction in the time spent on service location
- Improved accuracy due to real-time data integration
- Better user experience due to simplicity in navigation
- Efficiency in emergency situations
- Less dependency on using different applications
- Better decision-making due to relevant information provided

IX. LIMITATIONS

Despite its benefits, the system has some limitations:

- Dependence on internet connectivity for updates
- Accuracy of data relies on external data sources
- Privacy concerns related to location tracking
- High costs of development and running
- Scalability of the system for large amounts of data

X. FUTURE SCOPE

The future development of the platform can focus on several enhancements:

- Integration of Artificial Intelligence for predictive recommendations
- Implementation of voice-based interaction for accessibility
- Offline functionality for low network environments
- Integration with smart city infrastructure and IoT devices
- Use of machine learning for behavior-based recommendations
- Implementation of enhanced security mechanisms to protect user data

XI. CONCLUSION

The Smart Location Intelligence Platform provides a comprehensive solution to the challenges faced by users in locating essential services in unfamiliar environments. By integrating real-time data processing, intelligent filtering, and user-centric design, the system significantly enhances travel efficiency and overall user experience.

The platform not only reduces search time but also improves accessibility and decision-making, particularly in critical situations. With future advancements in artificial intelligence and smart technologies, the system has the potential to become an integral part of smart city ecosystems, contributing to safer, more efficient, and more connected urban environments.

XI. REFERENCES

- 1] Google, "Google Maps Platform Documentation," 2024.

-
-
- [2] Waze Mobile, “Waze Navigation and Live Traffic System,” 2024.
 - [3] H. Samet, *Foundations of Multidimensional and Metric Data Structures*, Morgan Kaufmann, 2006.
 - [4] P. Krumm, “A Survey of Computational Location Privacy,” *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.
 - [5] M. F. Goodchild, “Citizens as Sensors: The World of Volunteered Geography,” *GeoJournal*, vol. 69, pp. 211–221, 2007.
 - [6] A. Küpper, *Location-Based Services: Fundamentals and Operation*, Wiley, 2005.
 - [7] S. Steiniger, M. Neun, and A. Edwardes, “Foundations of Location-Based Services,” University of Zurich, 2006.
 - [8] N. Eagle and A. Pentland, “Reality Mining: Sensing Complex Social Systems,” *Personal and Ubiquitous Computing*, 2006.
 - [9] X. Zhou, Y. Xu, and W. Chen, “Location-Based Services: Current State and Future Directions,” *IEEE Transactions on Intelligent Transportation Systems*, 2018.
 - [10] M. Batty et al., “Smart Cities of the Future,” *The European Physical Journal Special Topics*, 2012.
 - [11] A. Zanella et al., “Internet of Things for Smart Cities,” *IEEE Internet of Things Journal*, 2014.
 - [12] D. Guinard and V. Trifa, *Building the Web of Things*, Manning Publications, 2016.

USE OF ARTIFICIAL INTELLIGENCE IN CARDIAC ARREST

¹Manish Dubey, ²Saloni Basare and ³Nikita More

¹Assistant Professor, BVIMIT University of Mumbai

^{2,3}Student, BVIMIT, University of Mumbai

ABSTRACT

The death of an individual due to cardiac arrest is an extremely serious medical emergency. Unless a victim receives immediate medical assistance, they may die. Although there have been recent improvements in the ability of the healthcare system to respond promptly to patients, significant problems remain that continue to lead to unnecessary patient deaths. Some of these challenges include a long process of diagnosis, a lack of trained clinicians, and inequitable access to care sources. The most recent example of technology that may assist clinicians in assessing patients at risk is Artificial Intelligence (AI). This technology can help to identify the possibility of an arrest as well as help clinicians predict what may happen next. It can also provide real-time assistance to help clinicians make clinical decisions while managing a patient with a cardiac arrest. The following topics will be covered in this paper in order to demonstrate how AI can assist clinicians throughout every aspect of managing a patient with a cardiac arrest: early identification of patients at risk, managing patients in an emergency situation, performing resuscitation, and providing care to patients after an arrest. AI will also help to analyze ECGs, vital signs, laboratory tests, and electronic health records to help identify patients at risk of experiencing a cardiac arrest. Based on this information, AI will be able to provide estimates of how likely the patient will experience a cardiac arrest and provide recommendations for immediate treatment. Additionally, AI-created summarised patient data, treatment plans, and decision support will assist emergency responders and hospital staff in communicating about patient populations. This paper will also discuss the various challenges associated with implementing AI into clinical practice.

Keywords: Artificial Intelligence, Cardiac Arrest, Emergency Healthcare, Predictive Analytics Generative AI

I. INTRODUCTION

A sudden cardiac arrest (SCA) is a life threatening emergency, in which the heart stops functioning properly and can no longer provide adequate blood flow. Without immediate assistance from someone trained and qualified within 4 to 6 minutes after suffering an SCA, the brain can suffer irreversible damage and the person will, more than likely, die soon thereafter [1]. There have been many innovations to improve emergency medical service; however, SCA is still one of the leading causes of death worldwide. In the United States alone, approximately 350,000 civilians experience an SCA outside of a hospital each year, and the average chance of surviving an SCA outside of a hospital is only 8% to 12%. The likelihood of surviving an SCA within a hospital is greater than that of surviving an SCA outside of a hospital (approximately

20% to 25%) and is dependent on how quickly assistance is provided and the quality of treatment provided [2]. These statistics indicate a clear need for us to develop a means to identify SCA in the early stages, obtain assistance sooner, and increase the quality of the assistance that is provided. In order for today's healthcare systems (whereby hospitals collect and store large amounts of data), those responsible for providing care to persons with SCA have access to a significant amount of information related to the patient's heart (such as ECG readings, vital signs, laboratory data, and electronic health records); however, it is extremely difficult to visually analyze all of this data in real-time. Therefore, by utilizing artificial intelligence (AI), the completion of these tasks can be improved as they relate to the prediction of risk, timely decision-making, and the provision of the appropriate level of care. This paper examines how AI and generative AI, in particular, can be applied across the entire cardiac arrest care process, including early warning, emergency response and resuscitation, and follow-up and documentation.

II. SEASONAL IMPACT ON CARDIAC ARREST AND THE ROLE OF AI

Heart disease is impacted by what season it is year-round. There is an increased incidence of cardiac arrest based on seasonal variation. Seasonal variations significantly correlate with the total number of heart disease-related deaths. Therefore, artificial intelligence will also play a key role in understanding how the incidence of cardiac arrest correlates with seasonal variation.

Studies reveal that climate-related fatalities due to heart disease occur at a rate of about

10 to 20 % of all deaths from heart disease in this country during the winter months. Cold-weather leads to a constriction of blood vessels and a rise in blood pressure (between 5 and 30 mmHg in extreme cold temperatures) which puts added pressure on the heart because of the additional demands placed on the body by cold weather. Furthermore, during the winter months people have a higher incidence of respiratory illnesses, less physical activity and less access to medical services.

Artificial Intelligence (AI) currently tracks an individual's ECG, heart rate, oxygen saturation, and blood pressure in real-time with the assistance of machine learning. Machine Learning analyses these metrics as they occur in real-time and can identify problems before they worsen. These systems are beneficial during periods when there is a higher risk of severe weather.

III. LITERATURE REVIEW

AI has made significant advancements in heart care applications. Models for identifying irregular heart rates from ECG can achieve between 85% and 98% accuracy [3] and provide physicians with an early warning system to assess a patient's risk of having a heart attack while in the inpatient setting, with accuracy rates exceeding 80% in some studies .

AI-assisted CPR devices have improved the quality of chest compressions by 20-30% [1]. AEDs (automatic external defibrillators) have been estimated to have a 95% or greater sensitivity in detecting shockable rhythms [1].

Generative AI tools assist physicians with documenting notes about their patients, communicating with them, reducing the time spent on paperwork by up to 40%, and improving organization [4]. However, concerns remain about protecting patient data from exposure, bias in data, distrust of technology by clinicians, and regulatory consent [5].

IV. PROBLEM DEFINITION

With all of these advancements in technology there is still an immediate need for assistance within five minutes after an individual has experienced cardiac arrest

.The primary challenges include:

- Failure to recognize initial symptoms in a timely manner.
- Lack of ability to synthesise a multitude of varying types of patient information.
- Difficulty at times, of finding Emergency Medical Service (EMS) personnel that have received formal training to manage cardiac arrest patients.
- Poor quality of CPR performed in many cases.
- Ethical & legal issues around the use of AI.

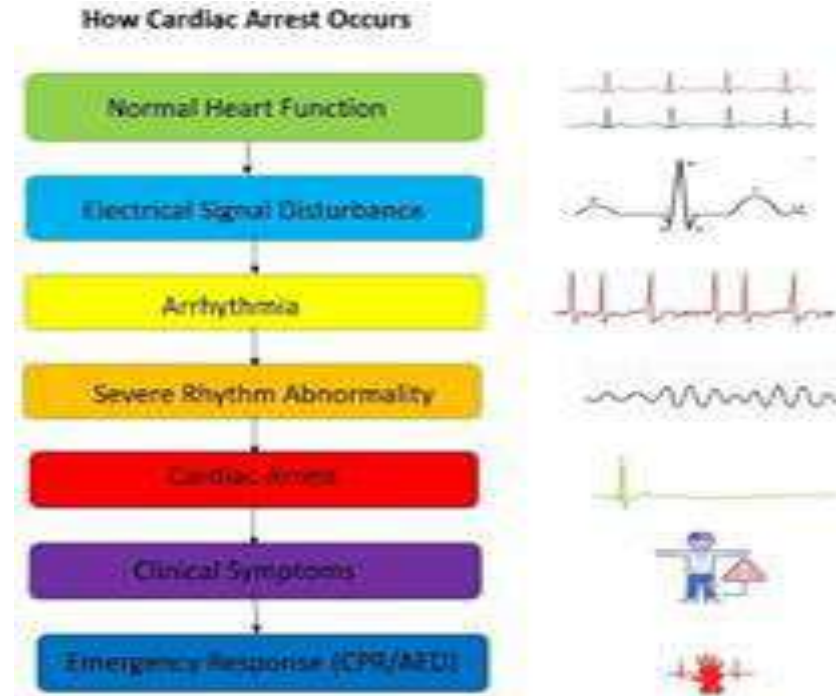
The operating costs are also very high due to excessive costs of implementing AI systems, the incompatibility of AI systems to existing infrastructure in the greatest proportion of locations where there is little to no income, and a desire for most of AI products to be fully automated (i.e. user friendly/cost-effective/understandable).

V. OBJECTIVES

This study aims at the following objectives:

1. To evaluate AI utilization at each stage of a cardiac arrest patient's treatment
2. To examine the employment of AI tools designed to warn or trigger heart attacks
3. To analyse the use of AI for CPR and defibrillation
4. To explore how Generative AI can contribute to emergency response communications and documentation
5. To define the ethical, logistical, and practical factors relating to the use of AI.

VI. MECHANISM OF CARDIAC ARREST



The heartbeat halts suddenly in this context. The heart usually works well on its own. The flow of blood through blood vessels occurs naturally with the functioning of each heart beat. Each heart beat is made up of an electrical signal. Electric signals are essential for the adequate functioning of blood flow to every body part, including the heart.

From time to time the electrical signals of the body become out of sync. This often occurs due to damage to the heart, blood vessel blocks or other types of health problems. Due to the out-of-sync electrical signals, the heart attempts to beat again, however it does so in an irregular manner. Thus, the clock-like balance of the previous heart beat is altered. This phenomenon is referred to as an arrhythmia.

Without the heart pumping blood continuously, blood circulation ceases, resulting in the cessation of all body functions; this is also known as ‘arrest’ or complete cessation of function.

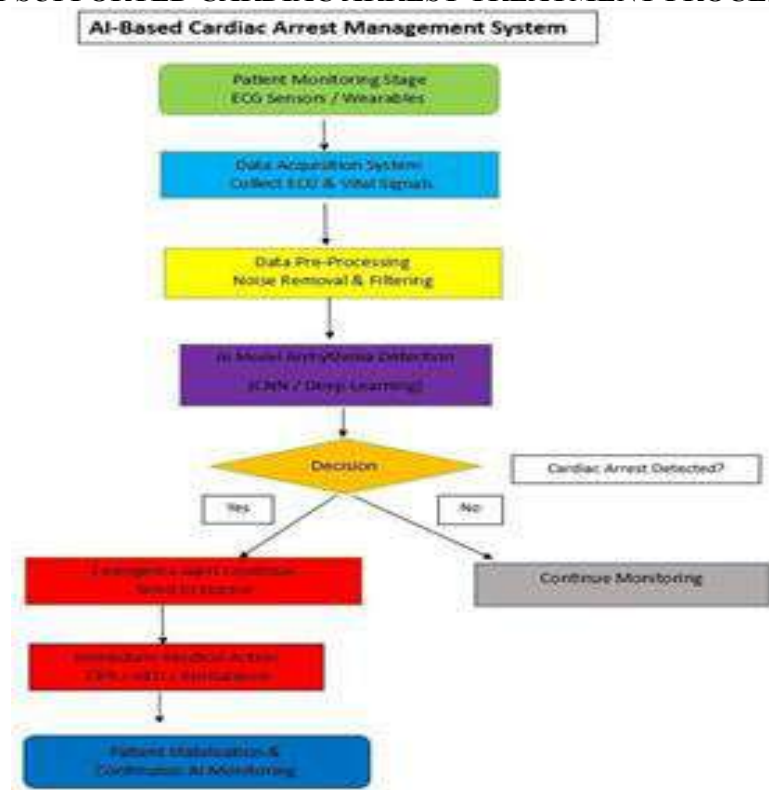
The sudden cessation of breathing is often referred to as ‘collapse’ and can be very scary for witnesses because it can be a life-threatening event; an individual does not

exhibit any signs or symptoms prior to collapsing, therefore, as soon as they become unresponsive, assistance should be obtained immediately for the collapsed individual. An unresponsive individual requires immediate assistance as they have ceased all respiratory functions. Medical responders employ techniques such as CPR, which

involves applying pressure on the chest in an effort to revive or restore essential body functions (vital).

Medical responders may also employ an AED, an electronic device that can deliver an electrical shock for the purpose of an attempt to restore normal rhythm/heartbeat; therefore, it is important to note that both CPR and AED are effective when used individually or collectively.

VII. AI-SUPPORTED CARDIAC ARREST TREATMENT PROCESS



At the outset, we monitor the patient's heart activity constantly via the collection of heart data from either sensors or wearables. The heart data collected will be transmitted to a computer, which will save and store this heart data for future review. This system will filter out excessive noise from the data collected, thus improving the overall quality of heart data collected, allowing for greater accuracy for future heart data collected.

Once filtered, data is then analysed via a computer program, which has a high capability of determining various forms of heart rhythms. The results provided will be utilised for the system to provide an appropriate response.

If the system detects an abnormality in the heart data, the system will issue an immediate emergency alert to the physician, enabling the doctor to provide appropriate treatment, such as performing CPR on the patient, or summoning an ambulance.

If no abnormality is detected, the patient's heart will be monitored continuously and in real time until the patient has been treated. Once treated, patient will continue to be monitored in order to confirm the stability of their heart, and to prevent any further difficulties.

VIII. ROLE OF GENERATIVE AI IN CARDIAC ARREST MANAGEMENT

A. Clinical Documentation

Generative AI's ability to automatically create structured clinical documentation eliminates the need for manual documentation by a clinician. Research indicated approximately a one-third reduction in documentation time associated with using generative AI for producing clinical documentation from existing information and resources [4].

B. Emergency Communication

Machine-generated summaries of essential information about a patient will make it easier for both ambulance personnel and hospital personnel to share concerns or issues regarding a patient, resulting in decreased errors during transfer of caring responsibilities [4].

C. Clinical Decision Support

Large Language Models (LLMs) will provide assistance to medical professionals during urgent circumstances by giving them recommendations for treatment options using established guidelines while identifying potential medication risks (e.g., drug interaction dangers) that may not have been considered during the course of medical treatment provided to a patient [4].

D. Training and Simulation

Generative AI will create realistic simulation training scenarios for mixed-use healthcare teams to enhance preparation in case of a heart failure event [4].

IX. ETHICAL, LEGAL, AND PRACTICAL CONSIDERATIONS

Fairness in Artificial Intelligence algorithms is largely reliant on diverse health records in the learning process of the model. The legal constraints surrounding personal health data must also be strictly adhered to, as must the effective protection of patient confidence, i.e., based on the use of these algorithms.

The final decision regarding treatment for patients remains with the healthcare provider and not with Artificial Intelligence as an independent entity [5].

Understanding how algorithms operate provides better assurance to both physicians and patients regarding their care as the reasons for Artificial Intelligence decisions become clearer and thus, allows for more confidence in treatment.

X.

XI. LIMITATIONS

The most Artificial Intelligence (AI) applications need extensive medical data and powerful systems to operate effectively. When the data used to train these algorithms is primarily from one demographic, the predictions generated may be inaccurate for other groups.

The significant expense of implementing such systems forces many healthcare professionals to be apprehensive about using them but because most clinicians spend so much time distracted, relying too heavily on machines for diagnosis or treatment may create significant medical errors that go undetected until after they occur. Therefore, while one major barrier to obtaining clinical AI solutions is clearly related to the cost of implementation, the second barrier is the resistance by most healthcare providers to change their traditional practices.

XII. FUTURE SCOPE

Future research should focus on:

Building Artificial Intelligence Models that are easy to understand is very important. We need to make Artificial Intelligence Models that people can understand.

We have to do some studies to make sure these Artificial Intelligence Models work well in life. This is necessary to check if the Artificial Intelligence Models are good.

We should also combine types of data, such as pictures and genetic information to make the Artificial Intelligence Models better. The Artificial Intelligence Models will be good if we use types of data like pictures and genetic information.

It is also crucial to make Artificial Intelligence systems work in places where resources are limited like some hospitals. Artificial Intelligence systems have to work in hospitals that do not have a lot of resources.

We have to make sure the rules that govern Artificial Intelligence are strong around the world. These rules are necessary for Artificial Intelligence to work everywhere.

Fresh progress in devices that people wear on their bodies along with the ability to process information on these devices could change how Artificial Intelligence keeps an eye on things. When these devices get better Artificial Intelligence might be able to track things in our daily life.

This is an interesting idea because Artificial Intelligence could really make a difference in our life. Artificial Intelligence can make our life better if we use it correctly.

XIII. CONCLUSION

Cardiac arrest is a global health concern. The chance of survival for individuals who undergo a cardiac arrest in a non-hospital setting is substantially lower, with less than 15% surviving to discharge. Artificial Intelligence (AI) and Generative AI technologies can improve early identification of cardiac arrest and assist emergency responders in providing timely interventions. Artificial Intelligence also assists

healthcare providers in the resuscitation of cardiac arrest victims as well as providing efficient care to such patients after resuscitation has been achieved. Artificial Intelligence does not replace physicians and nurses, but rather supports medical professionals in making clinical decisions with greater accuracy, resulting in less incidence of errors providing care. With careful, proper construction of the Artificial Intelligence system, along with proper implementation and testing, the potential for saving tens of thousands of lives annually exists. The application of Artificial Intelligence has great potential to enhance healthcare delivery. The potential benefits of Generative AI and Artificial Intelligence technology offers great opportunity to improve delivery of care for cardiac arrest victims.

REFERENCES

- [1] American Heart Association, “2020 AHA Guidelines for Cardiopulmonary Resuscitation and Emergency Cardiovascular Care,” 2020.
- [2] S. Girotra et al., “Trends in Survival after In-Hospital Cardiac Arrest,” *New England Journal of Medicine*, 2012
- [3] P. Rajpurkar et al., “Cardiologist-Level Arrhythmia Detection with Deep Neural Networks,” *Nature Medicine*, 2019.
- [4] A. Singhal et al., “Large Language Models Encode Clinical Knowledge,” *Nature*, 2023.
- [5] World Health Organization, “Ethics and Governance of Artificial Intelligence for Health,” 2021.

IPFS CONTENT ADDRESSING WITH BLOCKCHAIN VERIFICATION

¹Abhishek Yewale and ²Dr. Suhasini Vijaykumar

¹Master of Computer Application (MCA) Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

²MCA Department Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

ABSTRACT

Assessing the authenticity and integrity of online documents is an issue that is prevalent among universities, companies, and individual persons. This is more so when files are exchanged across systems and long durations of time. The conventional approaches normally rely on central databases or manual verification. The strategies are susceptible to manipulation, possess single points of failure, and are based on trust within a governing entity.

This project comes in with a decentralised document verification system where content addressing is performed using IPFS and verification is performed using blockchain. Within this system a document is converted into a cryptographic fingerprint and is stored on IPFS that generates a content identifier (CID). A smart contract is then used to record the CID together with the metadata required. The process generates a time-stamped record that cannot be changed and can be verified by anyone.

In the verification, the user reposts or chooses a document. The system then calculates its hash/CID and compares it with the record on-chain. This proves the authenticity of the document against the original document. The tool has a web-based interface, which assists in the major tasks such as uploading, verifying and managing the documents, which are quite easy to use by non-technical users and at the same time, the process is transparent and traceable. The system is developed to create trust in document exchange by decoupling storage and verification, where IPFS is used to store distributed files, and blockchain is used to establish secure audit trails, minimising reliance on centralised intermediaries.

Index Terms—InterPlanetary File System (IPFS), Content Addressing, Blockchain, Smart Contracts, Document Verification, Data Integrity, Tamper Detection, Decentralised Storage, Hashing, Provenance.

I. INTRODUCTION

Creating and sharing documents digitally has grown rapidly and has made it easy for people to create and share documents such as: academic certificates, identity proofs, medical reports, and organizational records. At the same time it has been easier than ever to alter a file without making visible changes, create a fake copy of an authentic document, or present an older version of a document as being the most recent version. A lot of organizations still use a centralised database, confirm/verifying an identity via email, or have manual verifications/confirming from the issuing agency to

verify identification. The limitation to these verification methods are practical in nature: they can take time to verify, may not be available after hours, and rely on one organization to accurately and securely maintain records. One of the major conditions of document authentication is the integrity verification that is ensuring that the file that is received is identical to the original one that was issued or uploaded. Conventional solutions usually keep documents in centralized servers and restrict access with the help of access checks. Nevertheless, such problems as server intrusions, insider threats, unintentional deletions, or unauthorized modifications may undermine trust in documented documents. Moreover, in cases of multiple participants having to read the same record, e.g., a recruiter reviewing a certificate, it is difficult to have it verified in a clear manner without revealing the whole document store.

This issue can be dealt with in a better way using decentralized technologies as they are the only way to have a better basis of trust for this issue. IPFS (InterPlanetary File System) is a good example of how content can be stored using a content-addressable way, in which files are identified by their cryptographic digest rather than where they reside on a storage medium. If any minor changes are made to the document, then that document will generate a different identifier. Therefore, you could use IPFS to verify the integrity of documents or to find a particular version of a document. IPFS alone does not provide a way to confirm if the identifier has been officially endorsed as corresponding with a valid issuer; at best it will provide assurance that the content then retrieved corresponds with the identifier that was provided.

To eliminate this deficiency, blockchain may be used as an irrevocable public register of document fingerprints registration.

The system can use a system on-chain, through smart contracts, to provide a tamper resistant, time-stamped attestation that a given document was in a particular form at a particular time. The subsequent attempt to introduce an amended version can be spotted by the new calculation of the content identifier and comparison with the generated value that was deposited on the blockchain. This integration separates duties: IPFS is distributed to control storage and retrieval and blockchain is used to offer integrity evidence and auditability. The web application I created provides all of the functionality necessary to upload, register, and verify documents as part of complete workflow. I chose to implement this system using content addressing with the InterPlanetary File System (IPFS) in conjunction with verification through the use of blockchain technology. The design goal for this application is to make it

easy to use for those who are not technically minded while still providing verifiable cryptographic correctness during verification.

Some of the key features included in this solution are a user selection of the document(s) to be uploaded; a content-based fingerprint generated by the application; registration on the blockchain by using a smart contract; and verification by

comparing the computed fingerprints to those recorded on the blockchain. By allowing verification to occur without the need for an external, centralized authority's database when the verification is performed, the system provides greater transparency and improves confidence in exchanging digital documents.

II. RELATED WORK

Decentralized technologies have allowed for the development of new storage systems that are both distributed and validated by the blockchain. Traditional storage methods involve using centralized servers; therefore there are a number of problems associated with this form of storage including data tampering and unauthorized access to stored data. Because of this researchers are looking at the use of decentralized solutions for file storage e.g., the interplanetary file system (IPFS) in conjunction with blockchain technology to improve data integrity and trustworthiness of their systems.

InterPlanetary File System (IPFS) is a decentralized (peer-to-peer) file system that are created to store and share data without a central authority. In contrast to location-based addressing of the common storage systems, IPFS uses content addressing, in which files are named by a cryptographic hash of their contents. The approach will make tampering with the data more readily identifiable because a new hash is created whenever the data is altered. Some of the studies have identified the benefits of IPFS that include enhanced scalability, reduced dependence on centralized infrastructure, and enhanced data accessibility.

However, although IPFS offers good results in terms of decentralized storage, it does not necessarily mean that it will be possible to verify the authenticity of data and ensure that its owners are recognized. In an attempt to fill this gap, scholars have proposed the movement of blockchain technology together with IPFS. Blockchain provides a ledger that is tamper proof and its records of transactions are stored in a decentralized and immutable manner. By recording hash values of files on IPFS in the blockchain, systems can prove the authentic original content any time without a trusted third party.

Several frameworks have reviewed the utilization of blockchain and interplanetary file system (IPFS) together as a way to secure data storage through the use of a smart contracts (verification of file integrity prior to download). For example, one system utilizes only the metadata in the blockchain as well as the content hash on the blockchain to lower costs and facilitate efficiency. In addition, some studies suggested that smart contracts could be used to automatically verify the integrity of a file prior to a person accessing it or downloading it.

While these methods have increased data security and data transparency, issues remain with performance optimization, verification speed and scalability. Many implementations focus only on either storage efficiency or on the security of the blockchain with little focus on both areas. Therefore, a combination of IPFS with

blockchain verification will provide a viable alternative for creating secure, distributed and immutable data storage systems.

The proposed system is based on the current researches by storing files via IPFS (decentralized storage) and storing and verifying content hashes via blockchain technology. This will make files resistant to changes and verifiable but will not affect the efficiency and scalability of distributed storage.

III. METHODOLOGY

The proposed solution incorporates Blockchain Technology and the InterPlanetary File System (IPFS), offering a way to store digital assets that can be verified and is decentralized. The main goal was to ensure secure storage, preserve the integrity of digital assets, and enable tamper-proof verification through the use of Content Addressing and Distributed Ledger Technology (DLT). The solution involves four key steps for implementation: uploading the digital asset, generating a hash for the asset, verifying the asset on the blockchain, and retrieving the digital asset once the verification is confirmed.

A. System Architecture

The architecture of the system integrates decentralised storage and blockchain validation. IPFS is the distributed storage layer which files are stored in a peer-to-peer network. The uploaded files become unique cryptographic content identifier (CID) depending on their contents. This CID serves as the fingerprint of the file and secondly it guarantees any alterations on the data result in a different hash.

On the blockchain, the blockchain network is a verification layer. Rather than saving the full file onto the blockchain, just the generated CID and relevant metadata are saved through smart contracts. This way, the size of the information required to store will be smaller than if it were stored in full, and it allows for the verification of the integrity of the data that has been stored to occur at any point in time.

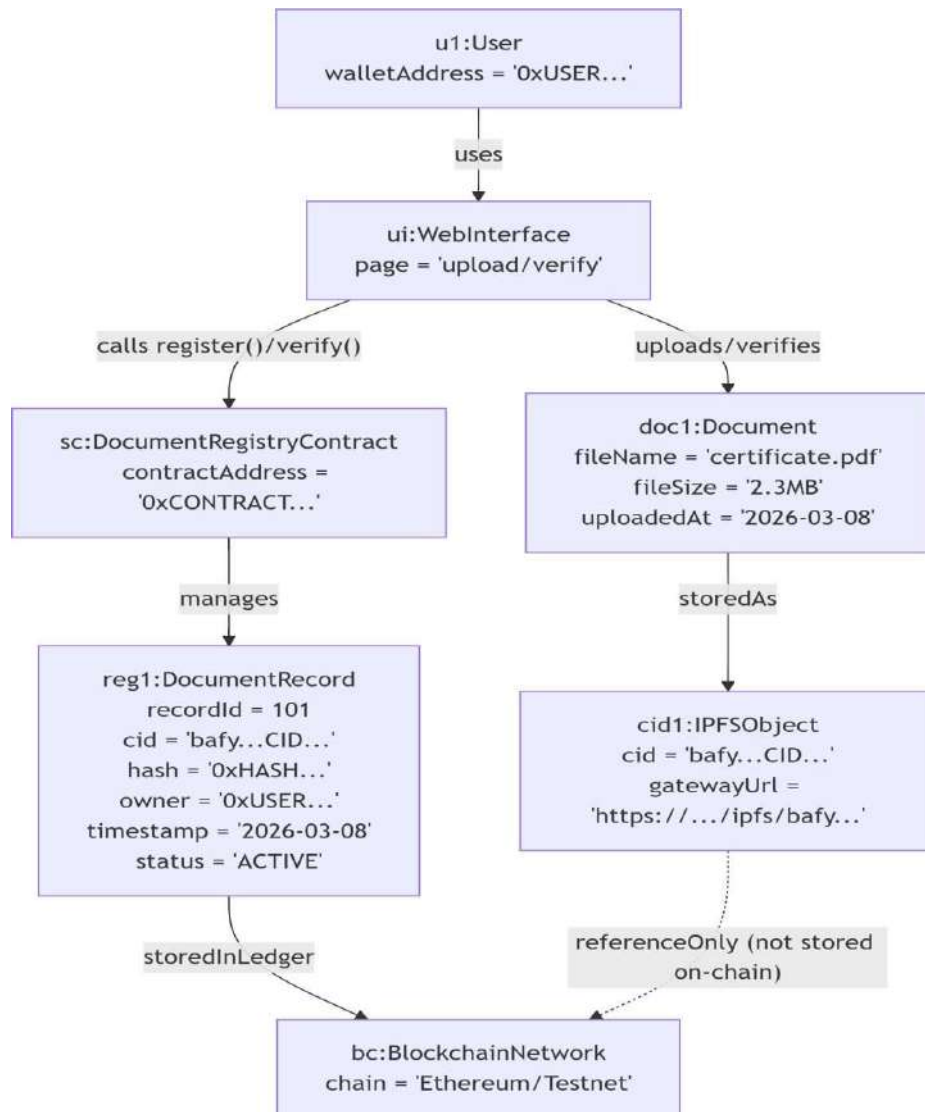


Fig. 1. IPFS Content Addressing with Blockchain Verification

B. File Upload And Content Addressing

After generation of a CID, it is then stored on the IPFS network for future access via distributed nodes. The CID can later be used as a reference for retrieval of the file at such time in the future. Since the hash that was generated was based on the content of the file, if the file is to be modified it would produce a completely different CID hash from before; therefore, tampering can be easily identified.

C. Blockchain-Based Verification

After generating the CID, a smart contract is used to log the hash on the blockchain. The CID, timestamp of creation, and owner of the file also have to be recorded on the blockchain as it acts as an unchangeable ledger for these records. Therefore, once the hash is on the blockchain, it cannot be altered.

During the verification process, the system compares the CID it received when it retrieved the file from IPFS (Inter- planetary File System) to the CID that is on the blockchain to establish that the file has not been changed or corrupted if both CID hashes match and will be deemed to have been changed or corrupted if they do not match.

D. File Retrieval Section

In order to get a file that has been stored, the user will give the CID of the file. The IPFS network is then asked by the system to provide the file based on this identifier. After the file is downloaded, the system recalculates the CID and compares it to the one that is stored on the blockchain.

This verification process provides that file that has been retrieved is not interfered with in storage or in transmission. When the verification is perfect, the file is sent to the user, otherwise, the system notifies the user of the possible data integrity problem.

E. Security and Integrity Mechanism

Using IPFS and blockchain as an integrated method to increase the security of a system is made up of two key components. The blockchain serves to maintain the immutability and transparency of stored files, and IPFS serves to provide decentralised storage and efficient distribution for files and applications. When combined, IPFS and blockchain create a system that allows users to verify the authenticity of their stored files without having to trust a central authority, and prevent modification of those files.

The ability of this method to offer a secure, scalable, and decentralised method of storing data and providing verification of that stored data is of utmost importance for applications that require high trust levels and data integrity.

IV. RESULTS AND EVALUATION

The proposed solution was created for the purpose of investigating how effective a combination of decentralized storage with blockchain verification would be. The goal was to create a testbed to evaluate the storage, integrity verification and retrieval capabilities of an IPFS based solution.

A. System Functionality Testing

File upload, generation of content hash, blockchain recording and file retrieval are the basic features of the system that I tested in the initial phase of evaluation. The system was able to use the IPFS protocol to generate a unique Content Identifier (CID) when uploading each file. The CID was then stored in a smart contract on the blockchain, which ensured that the file reference would be stored in an immutable ledger. A good amount of files in different formats such as PDFs, images and text

files I re-uploaded to the system in the course of testing. Each file generated a different CID, which proves that the content addressing scheme of IPFS recognised files correctly by their data and not by the position where they are stored.

B. Data Integrity Verification

I retrieved the files using their corresponding CIDs from the IPFS network to verify the effectiveness of our integrity verification system. Once the files had been recovered from the IPFS Network, I computed an additional hash from each of these files and compared it to the corresponding types (CIDs) of their original stored CIDs on the blockchain.

When comparing the results of our experiments, I observed that when comparing two identical files, the calculated CID matched the CID stored in the blockchain. Thus, I could confirm that the integrity of the file is valid. However, in instances where a file was modified after it had been uploaded, the calculated CID is inconsistent with the stored CID. This indicates whether or not the content of the file is valid. Thus, our verification system is functioning as intended.

C. Performance Analysis

I analyzed the time it took to upload files, generate a CID, write the blockchain, and retrieve files to evaluate the system's performance. IPFS enabled users to retrieve files from the nearest node, resulting in consistent retrieval times even with many nodes in the network.

In addition, simply storing the CID on the blockchain drastically reduced storage costs relative to keeping entire files on-chain. This design creates scalability and significantly reduces transaction fees while still ensuring verifiability of data integrity.

D. Security Evaluation

Blockchain technology has increased the security of the storage system overall by providing an immutable record of file hashes (i.e., the cryptographic equivalent of fingerprints for files). When a blockchain record is confirmed, it is impossible to alter original data within that record. Therefore, any attempt to alter data will be easily detected during verification against the original hash held in blockchain.

By using IPFS in conjunction with blockchain, the risks associated with centralised storage systems — such as server outages or single point failures — are reduced. The proposed solution provides a means of securely storing data and providing verifiable evidence that the data is stored in a safe and easily verifiable manner.

E. Discussion

The experiment analysis demonstrates that IPFS with blockchain is a valuable method of storing and validating the data in a decentralised manner. The system maintains integrity of data rather than just ensuring the storage and retrieval is fast and easy. The system is safe and robust, yet it can be enhanced by improving the

network's performance and accelerating the blockchain transactions to have a large scale application.

The findings indicate that the suggested approach is an excellent means of constructing distributed storage systems that are secure and difficult to breach.

V. CONCLUSION

The research proposes a decentralized storage solution that leverages both IPFS and blockchain to achieve trustworthy and secure file management. Centralized storage systems created by traditional methods face problems like single-points failure, little or no transparency, and are susceptible to alterations of data once it is stored. The proposed system aims to solve these issues with the help of the following features of the two technologies; IPFS offers a decentralized approach to file storage, while blockchain assurance is provided by immutability and trustworthiness.

IPFS is used in the solution to store files and uses a method called content addressing to create a digital identifier for any file (also known as the Content Identifier or CID) through a cryptographic function (Hash). A record of the CID is then added to the blockchain through a smart contract, allowing for the safe storage and retrieval of files. To retrieve a file from IPFS and ensure its integrity, a user's computer or device compares the CID associated with the original file from the blockchain (i.e., the unique fingerprint of the original) against the CID calculated for the file after retrieval. The subsequent results of this comparison confirm that when IPFS and blockchain are combined, the outcome is a credible and assured mechanism for maintaining data integrity as well as assuring transparency and decentralization, two other characteristics once again harnessed within this model working together.

The proposed framework appropriately detects unauthorized modifications to stored files through this approach, as such any user wishing to validate the authenticity of a file needs only to verify its existence on the blockchain and does not need to rely upon the central entity responsible for such verification. Although the outcomes are promising, they can be improved in certain aspects. The system can be optimized into a large scale to support a bigger amount of data and better network performance to speed up file access. Also, more complex features of smart contracts like access control would be added

to enhance security.

In general, the suggested system indicates a possibility to integrate decentralized storage with blockchain-based verification, which will establish a secure, transparent, and tamper-resistant data management system that can be applied in current distributed applications. Although the outcomes are promising, they can be improved in certain aspects. The system can be optimized into a large scale to support a bigger amount of data and better network performance to speed up file access. Also, more complex features of smart contracts like access control would be added to enhance security.

In general, the suggested system indicates a possibility to integrate decentralized storage with blockchain-based verification, which will establish a secure, transparent, and tamper-resistant data management system that can be applied in current distributed applications.

VI. REFERENCES

- [1] IPFS, “IPFS Documentation,” Online. Accessed: 2026-03-08. [Online]. Available: <https://docs.ipfs.tech/>
- [2] Solidity, “Solidity Documentation,” Online. Accessed: 2026-03-08. [Online]. Available: <https://docs.soliditylang.org/>
- [3] MetaMask, “MetaMask Developer Documentation,” Online. Accessed: 2026-03-08. [Online]. Available: <https://docs.metamask.io/>
- [4] Ib3.js, “Ib3.js Documentation,” Online. Accessed: 2026-03-08. [Online]. Available: <https://Ib3js.readthedocs.io/>
- [5] PlantUML, “PlantUML: Open-source tool that uses simple textual descriptions to draw UML diagrams,” Online. Accessed: 2026-03-08. [Online]. Available: <https://plantuml.com/>
- [6] IEEE, “IEEE Conference Templates,” Online. Accessed: 2026-03-08. [Online]. Available: <https://www.ieee.org/conferences/publishing/templates.html>

MALWARE DETECTION USING MACHINE LEARNING

Dr. Suhasini Vijaykumar¹ and Anjali Manoj Singh²

^{1,2}Department of Computer Application, Bharati Vidyapeeth Institute of Management and Information Technology Belapur, Navi Mumbai, India

Today, malware is an enormous threat to the computer world. The computer world is everywhere; people use computers each day to learn, to work, to bank, to shop, and to communicate. Because of this increased reliance on computers, the number of cyber attacks against them continues to grow exponentially. Attackers search for weaknesses in systems to exploit; they create new variants of malware frequently to take advantage of these weaknesses. The impact of malware on users and businesses is severe. Malware can delete data, corrupt files and programs, and can also steal personal and financial information. The result can be the loss of money and privacy or the inability to effectively use critical services. Therefore, detecting malware is critical to the field of cybersecurity. Historically, antivirus programs have relied primarily on signature-based detection. With signature-based detection, existing files are compared against known malware signatures that are contained in a database. This form of detection is only effective on known malware; the current form of detection is not capable of detecting new variants of malware, and malware detection also fails if the code of the malware is modified. The authors of malware utilize encryption, packing, and obfuscation techniques to conceal their identity in order to evade traditional detection systems. This limitation of traditional detection systems has led to the creation of a new Malware Detection System called MalScanML. This new system uses a combination of Machine Learning algorithms with Static Analysis (the analysis of Malware without executing it). The implementation of Static Analysis has resulted in a safer process of identifying Malware. The implementation of Static Analysis on Windows PE files allows the extraction of vastly different types of information associated with each PE file. Subsequently, a Machine Learning model is used to classify each PE file, resulting in the identification of Malware. The authors of this research compared the performance of the following Machine Learning Models: Decision Tree, Random Forest, and XGBoost. The results of their comparison found that XGBoost provided the best performance. This study used a Flask-based web application as an implementation of the overall MalScanML System. This study has allowed the authors to gain valuable insight into the various ways that Machine Learning can be utilized in the field of Malware Detection.

I. INTRODUCTION

Computers and internet services are widely used in today's world. Almost every activity depends on digital systems. People use computers for education, business, communication, and entertainment. Because of this heavy usage, security problems are also increasing. Whenever a file is downloaded, copied, or opened on a system, the antivirus software automatically scans it. This scanning process checks the internal structure of the file. Basically, the antivirus compares the file's code with the

list of malware signatures stored in its database. Malware is one of the most common security threats. Malware includes viruses, worms, trojans, ransomware, spyware, and adware. These programs are created to damage systems or steal information. In many cases, malware is used to gain access to systems without permission. Malware attacks affect individuals as well as organizations. Antivirus software is commonly used to protect systems. Most antivirus tools use signature based detection. This approach works only for known malware. When attackers create new malware, antivirus software is not able to detect it. When malware code is changed slightly, detection fails again. Because of this, systems remain unsafe. Malware creators use different methods to hide malware. These methods include encryption, packing, and code obfuscation. These techniques make malware difficult to detect using traditional tools. Due to this, better detection techniques are required. Machine learning helps in solving this problem. Machine learning can learn patterns from data. Static analysis is useful because files are checked without execution. In this project, machine learning and static analysis are used together for malware detection.

II. BACKGROUND

Most antivirus softwares works on a simple idea. Most antiviruses check files using a method called as signature method. A signature is basically a specific pattern inside the malware's code. Whenever security researchers discover a new malware, its structure is analyzed by the security researchers and then the pattern is stored in their database. Over time, this database keeps growing because new malware variants are continuously getting discovered.

When a file is downloaded, opened, or even copied into the system, the antivirus automatically scans it. While this is going on as well there is a comparison between the structure of the file and known signatures. If a match is found, the file will be flagged as harmful and the antivirus will take action which could include deleting the file, preventing the file from running, or moving it to a quarantine area. Quarantine simply means isolating the file so it cannot affect the rest of the system.

This approach works quite well when the malware is already known. If malware's signature is present in the database, detection becomes very fast and accurate. However, this method was effective for many years because most threats were not getting changed frequently. Updating the database regularly was usually enough to stay protected.

However, the situation is different now. These malwares are constantly modified by the attackers. They rarely use the exact same version again. Sometimes they hardly make small changes in the code, such as changing some instructions, encrypting some parts of the program, or adding a few extra lines that do not change the main behavior of the malware.

Even though the malware still has the same damaging effects, its code pattern may look different from the previous version due to the slight modification made by the attacker. Because of this, the antivirus may fail to detect it since the new version does

not match any stored signature exactly.

This is one of the main limitations of signature-based detection. There is a significant reliance on historical data. A system may not recognize new malware or malware that has been altered until it is well established. The reason it is no longer suitable to rely solely on this approach in the current rapidly changing cyber environment.

To address this issue, researchers have begun examining their approaches with new techniques such as heuristic analysis and behavior-based detection. Previously, security systems detected viruses by comparing them to existing patterns; current systems are much smarter in performing their tasks. The older system would only focus on how the file looked in code form, while newer systems will focus on the actual behavior of the file. If a program starts deleting files out of the blue, tries to access confidential data, or modifies system settings without approval from the administrator, the system will classify this activity as potentially harmful, irrespective of whether or not it is a newly discovered virus. Modern security systems no longer rely solely on matching a file to an existing known virus; they will also monitor the program for any unusual or harmful behavior, regardless of whether it is an entirely new virus not previously found in the database.

In recent years, malware detection has improved due to machine learning technologies. Rather than only using fixed rules and signatures to detect malware, these systems are trained using large sets of known good and bad files. During the training process, the system will learn to recognize patterns, trends, and key features that are related to malicious activity. When a new file is then encountered by the system, it will compare the new file with what it has learned in order to make an informed decision regarding whether the file is safe or not. Because of machine learning's ability to train systems, new and innovative security systems are now more flexible and better equipped to find and identify both new and evolving threats. Suspicious files can be examined using either dynamic analysis or static analysis. Dynamic analysis entails running the file in a safe and controlled space so that experts can observe how it operates. Dynamic analysis allows you to see what the file actually does, but takes more time and resources to perform. However, static analysis does not execute the file, it instead looks for unusual or suspicious characteristics within the structure, code and other facets of the file. Static analysis is usually considered to be more secure and faster than dynamic analysis because the file is not executed when the analysis occurs.

III. OBJECTIVE

The primary goal of this project is to design and implement a functional software detection application using a machine learning approach. This application will use machine learning algorithms to analyze the characteristics of executable files. By performing static analysis, the application will be able to determine if an executable file is either malignant or benign. The intent of this project is to create an intelligent system that will be able to identify both currently existing as well as previously

unrecorded types of malware, as opposed to being completely dependent on an older signature-based method of identifying potentially harmful applications.

Another key aim of this research work is to identify relevant attributes from Windows Portable Executable (PE) files without executing them. The proposed system will employ static analysis to ensure the system's safety while analyzing potentially malicious files. The attributes employed to train machine learning algorithms include header details, section information, imported libraries, entropy values, and metadata. These things are used for detecting the presence of suspicious patterns in malicious files.

The project also intends to compare various machine learning algorithms like Decision Tree, Random Forest, and XGBoost to identify which one of these models performs better in terms of accuracy and efficiency. The comparison is done using performance metrics like accuracy, precision, recall, and F1-score. Identifying the best model is an essential objective to ensure effective malware detection.

In addition another objective of this project is to implement the trained machine learning model into a user-friendly web application using Flask. This enables users to upload executable files and get classification results in an easy and convenient way. This will provide additional functionality for use within the system.

In conclusion, this project's goal is to create a secure, efficient, and intelligent malware detection solution that addresses the deficiencies of current antivirus solutions and improves the overall state of cybersecurity.

IV. LITERATURE REVIEW

A. Limitations of Traditional Signature-Based Malware De-tection

Traditional malware detection methods depend on utilizing signature-based approaches. In a signature-based methodology, antivirus systems will check for links between execution files' databases containing the signatures of recognized malicious files. If a link is found, the file will be determined to be malicious. Signature-based detection techniques have worked successfully to determine if something is malware; however, signature-based methods have serious limitations.

One of the weaknesses of signature-based methods is their inability to detect newly developing malware versions. Criminals will frequently alter the code structure of their malware so that it will be unrecognizable to the analysis of most detection devices (changed just enough so that the malware will not match any of the previously created signatures). If small modifications have been made to malware, signature detection will be having difficult time responding to the rapid increase in the total number of valid signatures associated with malware.

B. Static and Dynamic Analysis Approaches in Malware De-tection

The two primary techniques for analyzing malware objects are static analysis and dynamic analysis. Static analysis reviews the structural components of executables

without having to run them. Various attributes of the executable itself such as the PE header, libraries imported into the executable file, sections in the file, and entropy values can all be assessed during a static analysis. Static analysis is deemed to be a less risky method of malware detection than dynamic analysis because no potentially malicious code is executed.

By contrast, dynamic analysis involves executing malicious files in a secure area, called a 'sandbox,' to observe what happens to them. The researcher can watch what the file does whilst it is running by monitoring how many system calls the file makes, how many files the file modifies and what type of network communication occurs. Dynamic analysis has more details on behaviours than static analysis, but it takes longer and requires more computing power. Sophisticated malware may also be able to detect and escape the sandbox while executing. As a result, there have been numerous publications focusing on the combination of static analysis techniques with intelligent detection capabilities to increase the efficiency and reliability of both techniques.

C. Application of Machine Learning in Malware Detection

The rapid development of artificial intelligence is bringing machine learning to bear on malware detection. Machine learning allows the detection of malware by using patterns learned from large datasets to identify suspicious files. This means that machine learning is capable of detecting unknown malware types that traditional signature-based methods will not detect.

Various machine learning algorithms have been applied to malware detection, including Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM) and Gradient Boosting (GB). These types of algorithms analyze features extracted from executable files and determine whether or not those files are benign or malicious. In addition to their algorithmic capabilities, these algorithms (for example RF and XGBoost) also benefit from an increased detection rate due to their ability to use multiple decision trees to analyze and capture complex data patterns. Therefore, the use of machine learning techniques is critical for the identification of unknown and emerging malware threats.

D. Bringing Together Machine Learning and Web-Based Systems for Malware Detection

There have been a number of studies that have shown that using ML (machine learning) models in conjunction with web-based systems is a way to create malware detection systems that can be accessed and utilized by users more easily. An example would be developing a system where a user can upload a file they suspect may be malware for an analysis could use web framework software such as Flask or Django to develop the user interface of the cloud-based system.

Once a user has uploaded the file using one of these systems, the file will be subjected to a series of static analyses to extract information from the file about its characteristics that can then be utilized as input into a previously developed (i.e.,

trained) ML model. That selected ML model will then classify the file as either "malicious" or "benign", and return the result to the user via the web user interface. By employing web-based platforms, ML models and static analysis tools, it is possible for the user to quickly and easily detect malware on their system in real time.

V. PROBLEM STATEMENT

In today's world, with the rapid evolution of technology, computer systems and internet services have become an indispensable part of our lives. People make use of computer systems for different reasons like communication, banking transactions, shopping, education, and business processes. Along with the evolution of computer systems and internet services, the risk of cyber attacks is also on the rise. Among all the cyber attacks, malware is considered to be one of the major cyber attacks that can destroy computer systems, steal sensitive information, and disrupt the normal functioning of computer systems.

Traditional antivirus software uses signature-based detection techniques to identify malicious files. In this method, files are scanned and compared with the database of malware signatures to identify malicious files. This method is considered to be effective against malware attacks, but there are several disadvantages associated with this method. Cyber attackers often change their malware to create new variants of malware that can evade detection by signature-based detection techniques. Even a slight change in the malware code can change the signature of the malware and allow it to evade detection by traditional antivirus software. Another major challenge is the increasing complexity and volume of the malware being produced daily. Cybercriminals use different techniques such as code obfuscation, packing, encryption, and polymorphism to hide the malicious behavior of the malware. Due to the use of such techniques, it is difficult for security systems to analyze the suspicious code. Moreover, the process of manual analysis is time-consuming, and the security expert has to be highly skilled, which is impractical for large-scale detection. In view of the challenges, there is a need for more intelligent and automated detection systems for malware. Machine learning is one such technique that can be used for the detection of malware. Machine learning is a promising technique for detecting the characteristics of the malware, which may not be easily detected by other security systems. By analyzing the features obtained from the executable files through static analysis, the machine learning technique can classify the files as malicious or benign.

Therefore, this project will be centered on the development of a malware detection system that will be based on machine learning. The system will be designed to detect potential threats through analysis of key features from Portable Executable (PE) file. By incorporating the detection model into a web based application the system will be able to offer a simple way for users to upload the file and determine whether it is safe or malicious.

VI. METHODOLOGY

The proposed system for detection of malware follows a systematic methodology which includes collection of the dataset, feature extraction, data preprocessing, training of the machine learning model, implementation of the system and evaluation of the system. The objective of methodology is to develop an intelligent system that can effectively identify the malicious executable files using the machine learning approach. Overall the methodology is effective for the detection of malware ensuring that the executable files are detected without executing the potentially harmful files.

In the first phase of the methodology, the dataset is collected which is essential for the training and testing of the machine learning model. The dataset includes the Windows PE files which may be malicious or benign. Malicious executable files are collected from publicly available datasets of the malware. Similarly the benign executable files are collected from the trusted sources. It is essential to collect the executable files as the machine learning model can effectively identify the differences between the malicious and normal executable files. In the second phase, the feature extraction takes place through static analysis. Static analysis means analyzing the executable files without executing them. Python-based libraries and tools are used to extract the most important features from the PE files. These features include information from the PE header, libraries used by the executable file, the total number of sections, the size of the sections, entropy values, entry point information etc. These features help to identify suspicious patterns that are usually seen in malware.

Once the feature extraction takes place, the next phase of the machine learning analysis follows. In this phase, the preprocessing of the data takes place. During the preprocessing phase, the dataset that has been extracted from the malware is cleaned for the machine learning analysis to take place. Any damaged or missing information from dataset is eliminated. Once the dataset is clean, it is formatted appropriately for the machine learning analysis to take place. Then dataset is split into training and testing sets with suitable ratio. Generally dataset is split into 80

In the fourth phase, different machine learning algorithms are used to train the malware detection model. In this phase, different machine learning algorithms like Decision Tree, Random Forest, and XGBoost are used to classify the executable files as malicious or benign. The performance of the models is compared to select the algorithm that provides the best accuracy.

Finally, performance of the trained models is compared to select the best model that can provide the best accuracy while detecting malware files. Different performance metrics like accuracy, precision, recall and F1-score are used to measure the performance of models. These performance metrics can be used to measure the ability of the model to accurately classify files as malicious or benign without any false positives.

Based on the performance of the models best model is selected as the final model that can be used to detect the malware files.

During the implementation phase the machine learning model developed during the training phase is integrated into a web application developed using Flask web application framework. Users can upload executable files to the web application, and the features are extracted and passed to the model to predict the malware classification, which is then displayed to the user through the web interface.

Finally system is tested to assess the reliability and usability of the proposed system. The accuracy of the system the time taken to respond to the malware, and the performance of the system are analyzed to assess the effectiveness of the proposed malware detection system through the methodology discussed above, which helps to develop a useful and efficient system to detect malware using machine learning algorithms.

VII. SYSTEM ARCHITECTURE

The proposed system for detection of malware follows a well structured system architecture that incorporates various aspects such as static analysis, machine learning models, and web-based application. The system aims to provide a secure and effective way to analyze executable files and classify them as either malicious or benign. The system architecture of the proposed malware detection system can be divided into three major components. These include the user interface component, the feature extraction component that incorporates machine learning models and the prediction output component. The user interface component of the system can be implemented as a web based application that incorporates the Flask framework. Using the web based application the user can upload the executable file that needs to be analyzed.

Once the file has been uploaded, the system carries out a static analysis on the executable file. Here static analysis implies analysis of the file without executing it and this helps to keep the process safe during the detection process. At this stage, key features are extracted from the Windows Portable Executable File format. These features are derived from the PE header information, imported functions, the number of sections, section size, entropy values, entry point information, and other information. Here, the extracted features are the characteristics of the files.

Once the features are extracted, the data is passed on to the machine learning module. In this stage, the data is analyzed through classification algorithms like the Decision Tree Algorithm, the Random Forest Algorithm, and the XG Boost Algorithm. These algorithms are already trained. They are then used for the analysis of the features. They identify the patterns that distinguish the malicious files from the normal files. Among the algorithms, the best one is selected for the prediction.

Then the prediction module processes the output from the model and identifies whether the file uploaded is harmful or harmless. This is sent back to the web application and displayed to the user using the interface. This allows the user to easily check the output without having to possess technical expertise.

In conclusion, it is clear that the system architecture utilizes static analysis,

classification using machine learning, and a web interface in order to create a useful tool in detecting malware efficiently. This architecture is safe to use in file analysis and allows users to easily access the tool if they want to check whether the file is harmful or not.

VIII. CONCLUSION

To identify malicious executables, our project includes an integrated malware delay mechanism for its malware delay mechanism that involves both static analysis and a machine learning approach.

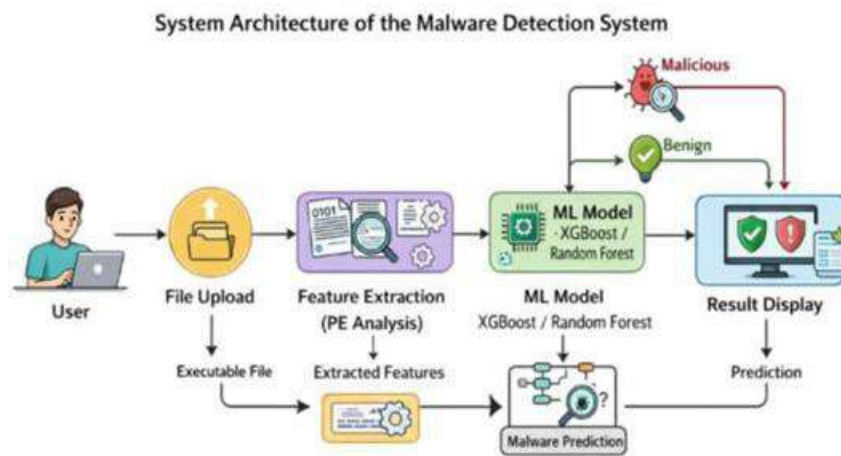


Fig.1. System Architecture of the Malware Detection System

Because our Detection mechanism processes Windows PE files without running them, this method is safer. This means that this can provide reliable results for the detection mechanism that analyses frequently used patterns by malicious executables using crucial features from the Windows PE file headers, imported libraries, sections, entropy values and metadata.

Various machine learning methods such as Decision Tree, Random Forest and XGBoost have been tested for their performance and efficiency in detecting malicious executables as evaluated by accuracy, precision, recall and F1 score metrics. Results demonstrated that XGBoost performed best overall for the detection of malicious executables with a higher overall accuracy.

This indicates that machine learning techniques can be used to detect malicious files more accurately compared to traditional techniques used to detect malware.

In addition to the machine learning model, the system was also implemented as a web application using the Flask web application framework, which provides the ability to upload executable files to the system for analysis. This provides an easier interface for malware detection and allows the system to be used by individuals who are not necessarily computersavvy.

Overall, the proposed system demonstrates the ability to leverage machine learning and static analysis to improve the malware detection capabilities of the system. It helps to alleviate some of the problems with traditional antivirus software, especially with respect to modified malware and malware the software has not seen before.

In the future, the system can be improved by adding larger data sets of malware, applying sophisticated methods such as deep learning algorithms, and adding dynamic analysis to check the files during their execution. Some additional features that could also be used to improve the system are: integration of real-time threat intelligence; automated reporting of malware; and cloud-based detection.

The proposed system is expected to offer a workflow that can effectively help in the detection of malware using machine learning techniques. This is done by first allowing a user to upload an executable file using the proposed webbased interface. After the file is uploaded into the system, static analysis is conducted on the file to retrieve important features from the Portable Executable file format, including the header information, section information, imported libraries, and entropy values. After the features are obtained from the uploaded file, they are then sent to the proposed machine learning module. In the module, the uploaded file is analyzed using the proposed Random Forest or XGBoost model to determine patterns that can classify the file as harmless or harmful. After the analysis is complete, the results are then displayed to the user using the proposed web interface.

REFERENCES

- [1] M. Schultz, E. Eskin, F. Zadok, and S. Stolfo, "Data Mining Methods for Detection of New Malicious Executables," *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 38–49, 2001.
- [2] U. Bayer, P. Milani Comparetti, C. Hlauschek, C. Kruegel, and E. Kirda, "Scalable, Behavior-Based Malware Clustering," *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2009.
- [3] I. Santos, Y. K. Penya, J. Devesa, and P. G. Bringas, "N-gram-Based File Signatures for Malware Detection," *Proceedings of the 11th International Conference on Enterprise Information Systems*, 2009.
- [4] K. Rieck, P. Trinius, C. Willems, and T. Holz, "Automatic Analysis of Malware Behavior using Machine Learning," *Journal of Computer Security*, vol. 19, no. 4, pp. 639–668, 2011.
- [5] S. Y. Yerima, S. Sezer, and I. Muttik, "High Accuracy Android Malware Detection using Ensemble Learning," *IET Information Security*, vol. 9, no. 6, pp. 313–320, 2015.
- [6] D. Ucci, L. Aniello, and R. Baldoni, "Survey of Machine Learning Techniques for Malware Analysis," *Computers & Security*, vol. 81, pp. 123–147, 2019.
- [7] M. E. Ahmed, A. Mahmood, and J. Hu, "A Survey of Network Anomaly

Detection Techniques,” Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.

- [8] S. Saxe and K. Berlin, “Deep Neural Network Based Malware Detection using Two Dimensional Binary Program Features,” IEEE Conference on Intelligence and Security Informatics, 2015.

AN INTELLIGENT IOT-BASED SMART HOME SECURITY SYSTEM USING REAL-TIME LOGGING AND LIGHTWEIGHT MACHINE LEARNING FOR ANOMALY DETECTION

Rajat Kshirsagar¹ and Vaishnavi Ingle²

^{1,2}Department of MCA, Bharati Vidyapeeth Institute of Management and Information
Technology Mumbai University

ABSTRACT

Smart technology for the home has grown exponentially with the evolution of (IoT) devices. Most low-cost security systems for the home are built upon straightforward rule-based triggers (i.e., triggering an alarm each time there is motion). Although these systems are relatively simple to implement, they generate a lot of false positives since they don't have the ability to distinguish between everyday household activity and authentic security threats.

In this paper, we describe the design and implementation of a smart security system for the home, which incorporates IoT sensors and a lightweight machine-learning algorithm for anomaly detection. The system uses an Arduino Uno microcontroller, to which is connected a PIR motion sensor, an MQ-2 gas sensor, and a keypad module for user authentication. All of the sensor activity readings and user interaction events are stored in real-time, so that a dataset capturing typical house behaviour can be created.

To identify how the dataset represents non-standard behaviour, we will train a decision tree algorithm on the dataset. Once trained, the algorithm is then converted to rule-based logic and uploaded to the Arduino, allowing real-time detection of anomalous behaviour, without having to rely on an off-site data centre. The system will alarm when anomalous behaviour is detected and can optionally notify users of an alarm through the use of a Wi-Fi module.

Experimental evaluations show that lightweight machine learning (ML) enhances detection accuracy and reduces false alarms compared to traditional rule-based techniques, while still conforming to the hardware constraints of an IoT device built on Microcontroller technology.

Index Terms—IoT, Smart Home Security, Arduino, TinyML, Anomaly Detection, Decision Tree

I. INTRODUCTION

The Internet of Things (IoT) has revolutionised the home by establishing an interconnection between devices/devices (such as appliances, lights, heaters and security devices) in the home to provide automated monitoring of their operation and execution and control of their activation. As it pertains to security at home, it is common for IoT applications to use different types of sensors (such as motion

sensors, carbon monoxide detectors, and smart locks) to send alerts to users regarding trespassing or potential hazardous conditions.

Most security systems that allow homeowners the ability to create their own installations and/or create customised forms of installations) that have been built using platforms such as Arduino use a simple set of rules to function—the most common being that if motion is detected, the system activates the alarm, and if the gas level exceeds a set amount, a signal is sent. These systems are simple to set up and operate, however they are not capable of understanding context. Therefore, the systems may alarm unnecessarily while a member of the household is conducting his/her normal daily activities in the household.

Current advances in machine learning for embedded devices are allowing for the running of very small machine learning models directly on low-power devices—many refer to this class of computing as TinyML—allowing microcontrollers to make intelligent decisions without the need for external servers or applications to make those decisions.

Therefore, taking advantage of the advances in machine learning systems, this paper proposes a power-efficient means to combine IoT sensing and LML (Lightweight Machine Learning) systems for improving the reliability of security monitoring in the home.

A. Problem Statement

Conventional smart home security systems (e.g., surveillance cameras, alarm systems) often operate based on pre-defined or static rules (e.g., a certain level of motion triggers the camera). This type of system is very easy and inexpensive to implement but does not take into account the variability of household behavior in real life (e.g., motion at night does not always imply someone is breaking into your house, whereas motion during the day generally does).

With traditional (static) rule-based systems, the inability to take into account contextual factors can lead to false alarms or failures to detect real threats. For instance, a motion sensor might detect motion while you are home late at night and therefore send an alarm signal to your surveillance camera, but a motion sensor may detect motion during the day and register that as normal. Thus, a rule-based system is not able to account for context when determining if the motion detected is suspicious or not. Another limitation common among many intelligent security systems is reliance on remote, cloud-based computing to process sensor data. Sending sensor data off-site to a remote server for processing adds latency, increases infrastructure costs, and may invoke user privacy concerns.

Accordingly, a new type of security technology needs to be created that is capable of performing intelligent anomaly detection locally on the smart home device itself. Such a new intelligent anomaly detection technology should be lightweight enough to run on resource-limited hardware while still capable of providing effective real-time monitoring of the home.

II. LITERATURE REVIEW

The last few years have seen an increasing number of studies that investigate the application of Internet of Things (IoT) technologies to enhance residential home security systems. Most such systems utilize microcontrollers, e.g., Arduino, and incorporate a wide range of sensors that are capable of measuring environmental changes and/or detecting potential security threats. Specifically, motion sensors (e.g., passive infrared (PIR) sensors) are often deployed to detect movement, while gas detection sensors can alert homeowners to possible gas leaks or the presence of smoke in their homes. Previous research has demonstrated that the integration of these sensors along with simple microcontroller-based systems will enable residential home security solutions that are both cost-effective and easy to implement. [1], [2].

However, most of the systems in the literature have relied on simple threshold-based or rule-based logic for alarm triggers. Examples of alarms include motion detection and crossing an arbitrary gas concentration level. The ease of designing and deploying these systems does come at a cost, as they are not able to use context or learn from previous activity data in their operation. This means that some of the normal household actions are going to set off an alarm that was not intended.

Embedded machine learning and TinyML have made it possible to execute smaller machine learning models on small low power devices like microcontrollers. [3]. The growth and advancement of these technologies brings us to an entirely new opportunity to develop more intelligent IoT systems. Algorithms that are lightweight, such as Decision Trees, are a good fit for these types of environments due to their low resource and memory requirements, while also delivering significant classification capabilities.

A. Research Gap

Although there are many different security solutions based on the Internet of Things (IoT), many of them still rely primarily on fixed rules to identify unusual activity within a home. Because of this, existing implementations do not adapt well to changes in a person's behavior and thus limit their effectiveness when used in the actual world.

Another typical limitation of current implementations is their use of machine learning services located within the cloud. While there are benefits to processing data in the cloud, there are also many disadvantages associated with processing data in this manner, such as increased latency, increased cost of operation, and potential privacy issues because data collected from sensors are sent to outside parties.

These two issues represent the need for a lightweight, locally developed anomaly detection mechanism that will run on edge devices so that intelligent detection can be performed on a microcontroller rather than requiring dependence upon the cloud infrastructure while providing an improved means of monitoring an area in real time.

III. SYSTEM ARCHITECTURE

This research included the development of an intelligent home security system that employs an arduino uno microcontroller as the main controller to receive input from various sensors and execute detection algorithms. The microcontroller uses inputs from a number of sensor devices to support the detection of different elements within a user's residence and for measuring temperature, humidity, light levels, etc.

A. System Architecture Description

The architecture shown in Fig. 1 follows a logical Sense– Process–Act flow. The design ensures that most of the computation is performed locally on the device while still allowing communication with external systems when necessary.

1) Input Layer (Sensing Unit): The sensing unit is the first part of the system and collects environmental and user interaction data. There are three types of input devices that will be used to monitor typical conditions related to the security of the home.

The PIR Motion Sensor is the digital eye that captures infrared images created by human movement. The MQ-2 Gas Sensor also continuously monitors the atmosphere around the sensor and checks for the presence of smoke or combustible gases. In addition to these two types of sensors, a 4×4 Matrix Keypad is used as the main way to interact with the sensor to allow authorized users to input authentication codes.

Both of these types of sensors provide analog and digital signals to the microcontroller. The sensors do not operate only as simple triggers; instead, the readings from the sensors are compiled and examined to look for anomalies that may indicate whether there is 'normal' or suspicious activity.

2) Processing Core (Arduino Uno): The Arduino Uno microcontroller is the main component of engine architecture and serves as the CPU or Main Processor for the entire system. It gathers input from all connected sensors and processes these inputs through embedded anomaly detection logic.

Unlike traditional Arduino-based systems where only simple rules are followed in an executing manner, this implementation follows a lightweight Decision Tree model created from a TinyML workflow. By aggregating all incoming sensor readings together, and applying the Rules of Decision created during training, the Arduino is able to tell if the detected activity is in normal condition or is likely to be an anomaly.

3) Output and Communication Layer: Once the processing stage is complete, the system responds by generating alerts or notifications depending on the detected condition.

- **Local Feedback:** New noises and lights can alert homeowners that an emergency has occurred; these alarms will allow the homeowner an immediate reaction to

emergencies where immediate action is required (e.g., gas leak or unauthorized access).

- External Notification: With the use of ESP8266 Wi- Fi module, the system can connect with other systems, including cloud-based services and mobile apps. Once an anomaly is detected, the ESP8266 will send notifications to the homeowner, allowing them to receive alerts regardless of whether they are present at their own home.

The core function of the system is preserved when using the ESP8266 module only for communications (since the primary decision making logic is embedded on the Arduino). The design also increases the reliability of the system by providing access to remote monitoring functions even when there is no longer a local internet connection available.

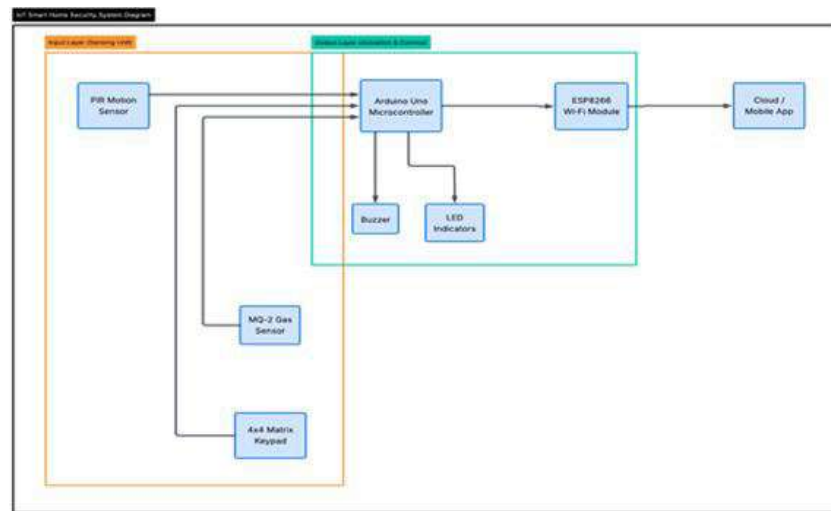


Fig 1. IoT Smart Home Security System Architecture

The system integrates multiple hardware components, each performing a specific function in the monitoring process:

- PIR Motion Sensor used to detect movement inside the monitored area
- MQ-2 Gas Sensor for identifying the presence of gas leaks or smoke
- 4x4 Matrix Keypad that allows authorized users to enter a security code
- Buzzer that generates an audible alarm when suspicious activity is detected
- LED indicators used to display system status
- ESP8266 Wi-Fi module that provides optional network connectivity for notifications

These sensors send data to be read by the arduino and also write down important events with a timestamp. Eventually, the data collected creates a miniature dataset that reflects how things are generally done in the home. This dataset is then used as part of the input for these models in order to detect any anomalies.

IV. METHODOLOGY

In order to develop the proposed system, multiple stages were completed: Data collection and preparation; Model training; and Real-time deployment to the microcontroller. A goal for the success of the project was to produce an anomaly detection solution which could be built using lightweight operations on limited resources of an embedded device.

Figure 2 illustrates the overall development lifecycle followed for building the TinyML-based detection model.

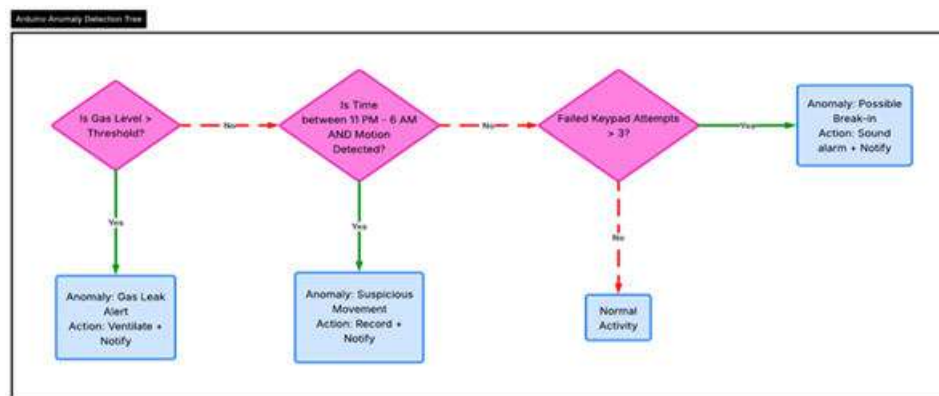


Fig.2. TinyML Development Lifecycle

At the beginning of the sample collection process, motion readings, gas levels, keypad activity and time stamps were recorded as a set of sensor events. These events were saved locally, or transferred to a system connected to the sample collection system where they were compiled into a dataset for subsequent analysis.

A. Feature Engineering

After the collection of the raw sensor data, an initial level of feature engineering took place, converting raw sensor readings into more insightful attributes. Features like time of day, frequency of motion events, number of keypad failure attempts and variations in gas sensor reading were derived, instead of simply using the raw value for these features.

These important features help to identify patterns that will allow for differentiation between normal household activity and potentially suspicious activities Fig 3 illustrates the value of the overall data flow and data processing steps used within this system.

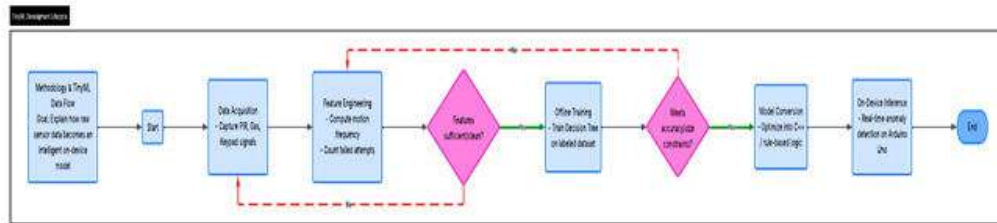


Fig.3. System Methodology and TinyML Data Flow

A Decision Tree model was trained with scanty sensor readings obtained from performing the workgroup to create an offline dataset of processed event recordings labelled according to normal or abnormal event types based upon the normal household activity patterns learned during data analysis.

Upon the completion of the training phase, the resultant model was converted to simplified behavioural rules that could be executed on the microcontroller (Arduino). The rule set was loaded onto the embedded or pre-programmed firmware of the microcontroller enabling it to make real-time inferences without relying on external computing.

B. System Workflow

There are many functional and operational processes involved in this overall system. First, we are responsible for monitoring all sensor data from all units; this is accomplished primarily through our Distributed Sensor Monitoring System. The next major step in our overall layout is anomaly detection and alert generation. Below summarizes the workflows of the various functional processes.

- 1) Collection of sensor readings from the PIR motion sensor, MQ-2 gas sensor, and keypad inputs.
- 2) Logging and basic preprocessing of the collected data.
- 3) Extraction of meaningful features from the raw sensor readings.
- 4) Offline training of a Decision Tree classification model.
- 5) Deployment of the trained model onto the Arduino microcontroller.
- 6) Real-time detection of unusual activity and triggering of alerts when necessary.

V. IMPLEMENTATION

A prototype of the new system was created with an Arduino Uno microcontroller, which is connected to various sensors and output components. The PIR motion sensor detects movement within the monitored area; the MQ-2 sensor monitors gas levels that could indicate a gas leak or smoke.

To allow authorized users to input a security access code, a 4×4 Matrix Keypad is provided. Unsuccessful login attempts are logged and will be used in determining the anomaly detection analysis.

The Arduino continuously reads incoming sensor data and evaluates it using the built-in decision tree logic developed from the training data model. The system analyzes the pattern of incoming sensor data, when detected, will determine if it is normal activity or potentially suspicious.

When any anomaly is detected, a buzzer will sound to give an audible alert. Additionally, the ESP8266 Wi-Fi module can send notifications over a network, if the user has enabled remote monitoring.

VI. EXPERIMENTAL SETUP

An Arduino Uno microcontroller was used as the central unit of a prototype system by integrating it with a variety of sensors and additional hardware that provide supporting functionality. Together, these items assist in monitoring both user and environment conditions in a home setting.

A. Model Efficiency and Hardware Constraints

It was essential to consider the efficiency of the machine learning model developed for the microcontroller based system, as the system has limited resources such as memory and processing power. A Decision Tree (DT) classifier was selected due to its low requirements for computing resources and its reliability for providing classification results.

By selecting a lightweight model, it is feasible to provide real-time detection on an Arduino Uno without relying on third party cloud services.

The major components of the hardware used in the experiment were described below:

- Arduino Uno (ATmega328P Microcontroller)
- PIR Motion Sensor
- MQ-2 Gas Sensor
- 4×4 Matrix Keypad
- ESP8266 Wi-Fi Module
- Buzzer and LED Indicators

Python and Scikit-learn were used to process the sensor dataset in preparation for model training. The Decision Tree model was trained, and then simplified to produce a rule set that could be directly embedded into the Arduino firmware.

Multiple tests were conducted to simulate normal household activities and simulation tests of potentially suspicious activity.

VII. EXPERIMENTAL RESULTS

Table I presents a comparison between the traditional rule-based system and the proposed TinyML-based anomaly detection approach. The comparison is based on commonly used classification metrics.

Table I: System Performance Comparison

Metric	Rule-Based System	Proposed System
Accuracy	82%	93%
Precision	78%	91%
Recall	80%	92%
False Alarm Rate	High	Low

The results indicate that incorporating a lightweight machine learning model improves the system's ability to correctly identify unusual events while reducing the number of unnecessary alerts.

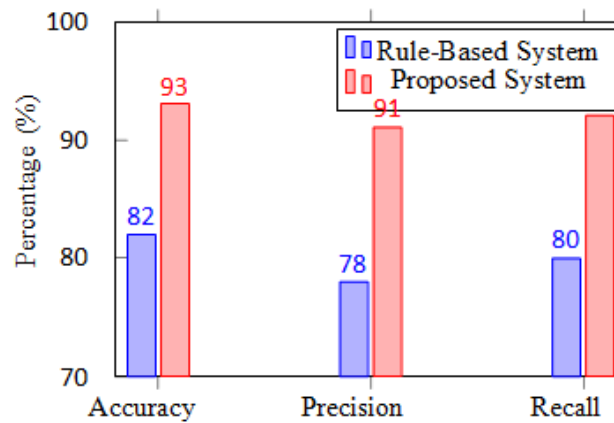


Fig 4. Performance Comparison between Rule-Based and Proposed TinyML System

A. Confusion Matrix

To further examine the model's classification performance, a confusion matrix was generated based on the results obtained during testing.

Table II: Confusion Matrix for Anomaly Detection

	Predicted Normal	Predicted Anomaly
Actual Normal	46	4
Actual Anomaly	3	47

From the confusion matrix it can be observed that the model correctly classified the majority of both normal and anomalous events, while maintaining a relatively low false positive rate.

VIII. EVALUATION METRICS

To evaluate the system, we utilized four core classification metrics. These provide a mathematical look at the trade-off between sensitivity and reliability:

- Accuracy measures the overall success rate:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

- Precision focuses on minimizing false alarms:

$$\text{Precision} = \frac{TP}{TP + FP}$$

- Recall ensures real threats are not missed:

$$\text{Recall} = \frac{TP}{TP + FN}$$

- F1-Score provides a balanced performance average:

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Here, TP and TN represent correct detections, while FP denotes false alarms and FN represents missed security events.

IX. RESULTS AND DISCUSSION

The system proposed here shows that it is possible to deploy lightweight machine learning models using IoT hardware which has limited resources. The proposed system effectively differentiates between household activities that are considered normal and those that fall under the category of suspect, using the patterns in the data produced by the sensors. The system correctly identified experimental scenarios such as detecting motion at night, having multiple attempts at using the keypad result in failure, and an increase in the level of gas in the house, as being examples of anomalous conditions. In addition, the proposed system was able to provide greater detection accuracy than would have been available through the use of more traditional rule-based systems while having very low levels of computational overhead. The performance analysis of the proposed system compared to the performance analysis of the more traditional rule-based system is provided in Figure 4.

X. CONCLUSION

A novel IoT-enabled Smart Security System for intelligent home security is proposed in this paper. The system focuses on real-time logging and lightweight machine learning-based anomaly detection with the use of low-cost, off-the-shelf hardware such as an Arduino Uno, PIR Sensors and MQ-2 Gas Sensors for monitoring

environmental activity in a household. The Decision Tree Classifier algorithm is trained using collected sensor data from the hardware and then implemented on the microcontroller to conduct real-time anomaly detection. Experimental results show that the Smart Security System greatly enhances accuracy of detection and provides less false alarms in comparison to traditional rule-based systems.

The research findings add to the growing body of knowledge about how TinyML can enable intelligent edge-based security systems for smart homes without high computing or power demands. Intelligent edge-based security solutions for smart homes may improve the safety of the home while protecting user privacy through reduced reliance on cloud-based processing.

REFERENCES

- [1] A. Smith, "IoT-Based Home Security System Using Wireless Sensors," *IEEE Access*, vol. 10, pp. 11234–11245, 2022.
- [2] J. Brown, "Smart Home Monitoring using Arduino," *International Journal of IoT Research*, vol. 5, no. 2, pp. 45–53, 2021.
- [3] P. Warden and D. Situnayake, *TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers*. Sebastopol, CA, USA: O'Reilly Media, 2020.
- [4] S. Kumar, "Gas Leakage Detection System Using IoT," *IEEE Sensors Journal*, vol. 21, no. 8, pp. 10234–10241, 2021.
- [5] M. Abadi et al., "TensorFlow: A System for Large-Scale Machine Learning," in *Proc. 12th USENIX Symp. Operating Systems Design and Implementation (OSDI)*, 2016, pp. 265–283.
- [6] L. Da Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.
- [7] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.
- [8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [9] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," *Cisco White Paper*, 2011.
- [10] H. Ning and H. Liu, "Cyber-Physical-Social Systems in IoT," *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 153–165, 2015.
- [11] R. Mitchell and I. Chen, "A Survey of Intrusion Detection Techniques for Cyber-Physical Systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

-
-
- [12] A. S. Sodiya, H. O. Onashoga, and O. B. Ajayi, "Towards Building Secure Smart Home Systems Using IoT," *International Journal of Computer Applications*, vol. 162, no. 2, pp. 15–20, 2017.
 - [13] B. A. Kitchenham and S. Charters, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," *Keele University Technical Report*, 2007.
 - [14] F. Chollet, "Deep Learning with Python," *Manning Publications*, 2018.
 - [15] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009.

HEALTHY FOOD: A SMART THALI-BASED PERSONALIZED NUTRITION RECOMMENDATION SYSTEM

¹Mansi Kumbhar, ²Dr. Suhasini Vijaykumar and ³Aaradhana Rajbhar

¹Master of Computer Application (MCA) Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

²Guide – MCA Department Bharati Vidyapeeth's Institute of, Management and Information Technology Navi Mumbai, India

³Master of Computer Application (MCA) Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

ABSTRACT

Lifestyle related diseases are posing a significant health hazard to the world; they are obesity, diabetes, high blood pressure, and heart disease. The primary contributor to such issues is the increased consumption of highly processed foods and convenience foods. The society is also losing education in regard to nutrition and healthy eating habits. Ample information regarding nutrition is found on the internet, and this is also applicable to information on dietary methods. Most of this information however is too complicated to be understood by the average person, and it is written at a level that may be hard to grasp. Moreover, it is hard to develop a nutrition plan that, on the one hand, should be considered practical, and, on the other hand, it should be possible to incorporate it into everyday life. This puts a definite requirement on dietary support systems. It is this that Healthy Food for Healthy People strived to address in a new manner. The team would take online strategies to establish a customized diet proposal framework, which is guided by advanced nutrition science and novel data-driven nutrition decision frameworks. The system will evaluate the caloric requirements of a user and will give personal meal recommendations depending on the entries made about the user in terms of age, height, weight, BMI, food preferences, and health aspirations. The Smart Thali System has been developed to be used in India, and is intended to serve available meals that are well balanced regarding the inclusion of carbohydrates, proteins, fats, vitamins, and minerals.

The system does not emphasize calorie counting as it does in most diet apps and rather emphasizes balanced nutrition, foods that are culturally favorable and the use of foods that are readily available in the local market.

Index Terms—Personalized Diet Planning, Smart Thali, Nutri-tion Informatics.

I. INTRODUCTION

Over the past years, obesity, diabetes, hypertension, and cardiovascular disorders have been some of the lifestyle-related diseases that have raised serious concerns in the world. The other major cause of the increase in the number of these health problems is the embracing of unhealthy eating habits and sedentary lifestyles. The process of urbanization, the hectic working schedule, and the growing popularity of processed and fast foods has had a great impact on the eating habits of people.

Consequently, this causes many people to not eat a well balanced diet, which is necessary to ensure good health and well being.

Though the extensive information regarding healthy diets and nutrition can be found on a variety of digital sources, not every human being can comprehend it and implement this knowledge into their functioning. The antique diet planning approaches usually require an excessive count of calories or complicated diet plans, which may be rather challenging to comply with regularly. Moreover, most of the available diet management applications are created with western dietary patterns and foodstuff in consideration, which can not be exactly compatible with the Indian cultural eating habits and food items that are locally available. This forms a disparity between nutrition principles and meal planning.

Balanced meal is also a traditional Indian concept, which is symbolized by the so-called Thali, which is a mix of cereals, pulses, vegetables, dairy products, and other nutritious food products. The meal set up inherently promotes the balanced distribution of nutrients by consuming carbohydrates, proteins, vitamins, minerals, and healthy fats in a predetermined manner. Nonetheless, people are not always aware of how to adapt these elements of foods according to their own health conditions, age, weight, and needs in nutritional terms.

In response to this issue, the proposed project is entitled Healthy Food for Healthy People and presents a web-based system of a personalized nutrition recommendation, which creates a Smart Thali, depending on the specific parameters of the user. The system gathers all the necessary user data including age, weight and dietary preferences and calculates them based on predefined nutritional standards to suggest a balanced meal. Also, the platform offers visual nutrition data to assist users in having a clearer insight into their dieting habits and nutrient profile.

The purpose of the suggested system is to make the process of planning the diet easier, encourage the adoption of healthier food options, and raise awareness about the balanced nutrition in a culturally appropriate way. Incorporating primordial methods of computation with nutrition, the system wants to facilitate preventive medicine and promote healthy eating habits in the population that are sustainable. The site is an illustration of how digital health technologies can help users make informed choices about their diets and have a balanced way of life.

II. PROBLEM STATEMENT

The changes in lifestyle have led to major transformations in the recent past. They have changed their eating habits and have created more consumption of fast foods. And as well as eating irregularities and reduced nutritional knowledge. The expertise to make a meal that contains a combination. A sufficient quantity of protein, carbohydrates, fat and vitamins is lacking in a lot of people. This has led to an increase in several age groups in lifestyle related diseases. Although there are a host of exercise apps, there are a hundred and fifteen dieting ones. Number of these apps contain Westernized food, the number of which counts. Calories, and diet plan that an average Indian

would never adhere to. The majority of such applications are paid through subscription, monitor everything, and need an understanding of nutrition, not the least of which is possessed by the majority of people. Students do not have. There is a tradition the Indian Thali hath. Is socially condoned as a way of a complete balanced meal. But the way of making a Thali is not all. As perceived by most people concerning the age of a person, his weight, and dietary needs. This explains why there is need to have a culturally accepted system. Easy, and simple instructions on how users can make a balanced. Indian meal. This is what makes it so in this project. A user-friendly and interactive platform is developed to help users. In the interpretation of nutritional data, creating well-balanced meal ideas and developing a web based solution to facilitate the. Encouraging healthy eating habits and preparation of a balanced meal.

III. LITERATURE REVIEW

Over the last few years, the growing popularity of lifestyle diseases like obesity and diabetes and cardiovascular disorders has resulted in substantial research on the topic of nutrition management systems and digital health apps. Different scientists have come up with smart diet advisory systems that make use of the computational methods to enable people to engage in balanced diets.

Trattner and Elswailer (2017) analyzed the evolution of food recommendation systems and emphasized the significance of individual nutrition advice based on data-driven methods. Their work proved that the recommendation systems may help users to choose more healthy meals based on their dietary preferences and nutritional needs. Equally, Elswailer and Har-vey (2015) investigated the prospects and issues surrounding food recommendation systems, stating that it is necessary to provide more individualized dietary advice and enhance user interaction.

A number of studies have additionally been dedicated to the creation of intelligent planning systems of diets. Sharma and Jain (2017) also suggested a system of diet recommendations that will produce an individual meal plan according to the health indicators of the user or age, weight, and lifestyle. The experiment showed that the rule-based recommendation methods may be effectively used to help people to adhere to balanced nutrition. Khan and Patel (2019) also gave this idea a further step by creating a smart diet planner with recommendation algorithms, which gives structured meal suggestions.

Digital health technologies in diet management have also received extensive research. Lee and Park (2018) studied the usefulness of mobile health apps in health lifestyle promotion. They demonstrated that the digital platforms can enhance the awareness of users about their nutrition and help oversee their diets.

In spite of these developments, most of the current systems of diet recommendation rely mostly on the counting of calories and the western patterns of diets. Such methods might not be entirely appropriate in areas where people have dissimilar cultural food practices such as India. The standard Indian meal system, which is

popularly referred to as the Thali, reflects naturally a balanced meal comprising carbohydrates, proteins, vegetables as well as dairy products. Nonetheless, such a culturally relevant meal structure is very scarcely integrated into the recommendation model of very few digital systems.

To fill this gap, the proposed system is aimed at producing individual dietary suggestions following the concept of Smart Thali, which corresponds with Indian dietary habits. The system will offer a convenient and sensible way of enhancing nutrition and adopting preventive healthcare by integrating user-feedbacks, rule-based advice, and nutrition analytics.

IV. OBJECTIVE

- **Main Aim:**

The primary goal of the project is to develop a web-based personalized nutrition recommendation system that integrates the concept of Smart Thali. This system will provide users with meal suggestions that are nutritionally balanced and encourage healthy eating habits.

- **Secondary Aims:**

1) User Data Collection and Profiling: Collect necessary user details such as age group, body weight, eating patterns, and health goals to create an individualized nutrition profile. .

2) Calculate the daily nutritional needs, including calories and the breakdown of macronutrients like proteins, carbohydrates, and fats, based on recognized dietary guidelines.

3) Smart Thali Generation: Create a well-designed Smart Thali that offers balanced Indian meal combinations from the food pyramid, including items like cereals, pulses, vegetables, dairy, and other food groups.

4) Nutritional Database Integration: Establish a detailed database of meal suggestions, containing the nutritional values of commonly consumed Indian foods.

5) Nutrition Analytics and Visualization: Offer users de-tailed analysis and visual aids such as bar charts to help them understand the distribution of nutrients in their diet and maintain a balanced eating pattern.

6) Rule-Based Recommendation Engine: Implement a rec-ommendation system that uses logical rules and user in-puts to provide meal suggestions in line with nutritional guidelines.

7) Awareness and Preventive Healthcare Support: Promote awareness of nutrition and preventive healthcare by en-couraging users to make informed and balanced dietary choices.

8) Future Development and Scalability: Design the system in a modular way to allow for easy integration of future features such as backend databases, machine learning, real-time tracking, and advanced personalization options.

VI. METHODOLOGY

The systematic approach of the suggested system is to make a web-based model of personalized nutrition recommendation system where balanced meal recommendation is achieved based on the concept of Smart Thali. The system has a systematic procedure that includes data gathering, parameter analysis, generation of recommendation and displaying the results.

V. MARKET SURVEY

As my study indicates, the mobile fitness and nutrition app market, which is one of the digital-gaming boom segments, has grown rapidly. Consumers are now able to download an app to keep tabs on calories, monitor meals, compute the BMI, and record physical activity, which makes them health-conscious. The majority of the trendy applications are aimed at the calculating of calories intake and expenditure to assist their users in meeting their weight targets. Nonetheless, there are a number of shortcomings with the apps that are currently in the market. To start with, most of the mobile fitness and nutrition applications are made to support the western dietary practices. This might not suit customers in India due to their eating habits, availability of various foods, and their cultures. The mobile applications that demand the user to monitor calories are also too complex, monotonous and unrealistic to the user. In addition, in most common mobile fitness and nutrition apps, the paid subscription option, which implies high-quality options, is unavailable to students and other users. The need of the user to have a balanced diet is also not properly taken care of in most of the mobile fitness apps. The app allows users to monitor their caloric intake, but gives the user the option of consuming an unbalanced diet due to the app not paying much attention to the ratio of the carbohydrates, proteins, and fats contained in the diet. Very few mobile nutrition and fitness also make the task of the user monitoring the food intake easier and inform the users about the basics of food tracking that negatively influences new users. Very few mobile nutrition and fitness also make the task of monitoring food intake of the user easier and teach the users the principles of food tracking, which negatively impacts new users.

Users require a platform that will recommend what to eat, and show users how to balance their nutrition in a straightforward and practical manner. Healthy Food for Healthy People is a system that targets culturally appropriate Indian eating habits, Smart Thali generation and uncomplicated nutritional feedback to fill these gaps. It is concentrated on preventive health and health awareness. It is a web-based, free and easy-to-use solution.

1) User Data Collection

The former is the process of first gathering the necessary user data, which includes age group, body weight and dietary preferences, with a user friendly web interface. Such parameters are required to know the health status and nutritional needs of the user.

2) Parameter Processing

The system then processes the user parameters to come up with the approximate nutritional needs after gathering the input data. The stipulated amount of macronutrients in terms of carbohydrates, proteins, and fats is estimated through simple rules and guidelines of nutrition.

3) Recommendation Engine- Rule-Based

The system is executed on a rule-based recommendation basis. The system uses established eating regulations to align user specifications with the food items. This will make sure that the recommended meals are well balanced in terms of nutritional content.

4) Smart Thali Generation

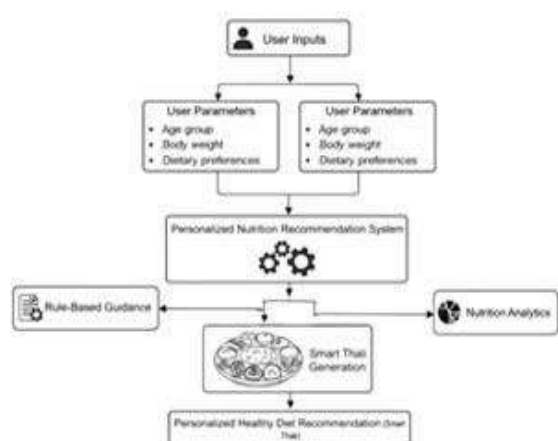
Depending on the estimated nutritional needs, the system produces a Smart Thali, which is an Indian meal balanced. The Smart Thali incorporates various types of food like cereals and pulses, vegetables and dairy products, and salads that are well balanced in the distribution of nutrients.

5) Nutrition Analytics

Other benefits of the system include the ability to offer graphical nutrition analytics to enable its users to grasp their balance in nutrition. The charts of the suggestions without having to track them manually and with a lot of data entry. The proposed

system is more concerned with nutritional balance and concrete meal plans compared to the traditional application that is based on calories.

Overall, the results indicate that the proposed Smart Thali-based recommendation system can be a useful instrument in guaranteeing healthy eating habits. Combination of customized recommendations, nutrition analytics, and culturally specific meal frameworks render the platform practical in different respects of education and preventive healthcare awareness. The effectiveness and the accuracy of the work of the system could be further improved with the implementation of machine learning algorithms, the enhancement of the nutritional information database, and the introduction of real-time tracking features in the future. Macronutrient distribution are viewed visually, which is easier to interpret the nutritional intake by the user.



6) Individualized Diet recommendation

The Smart Thali and nutrition insights created guide people to the making of more healthy food choices and a balanced diet.

Flow Summary:

User Inputs → Parameter Processing → Recommendation Engine → Smart Thali Creation → Personalized Diet Recommendation Output

VII. ANALYSIS AND FINDINGS

The analyzed proposed system was evaluated according to its capacity to produce individualized dietary guidance and offer balanced nutrition advice to the users. The site effectively takes user data including age group, body weight and dietary preferences to determine approximate nutritional needs and produce a Smart Thali recommendation. The analysis demonstrates that the system is very useful in integrating basic computational reasoning with nutritional principles to generate useful and culturally appropriate eating recommendations.

In the process of assessing the system, it was noted that the Smart Thali model assists users to know how various categories of food form a balanced diet. The system

contains ingredients like cereals, pulses, vegetables, and dairy products, which mean that the recommended meals are made up of the right amount of carbohydrates, proteins, and fats. The strategy makes it easy to understand the idea of balanced nutrition among users who might not have an idea of the process of dieting.

The other significant finding of the analysis is that the nutrition analytics module is helpful. The visual map of macronutrient distribution helps users to see at a glance their nutritional consumption and determine the potential deficiency in their diet. This aspect enhances the awareness of the users and promotes the consumption of healthier food.

The usability is also good since the system has a simple interface and is lightweight web-based. The user is able to input his or her information easily and get individualized

VIII. CONCLUSION

The project Healthy Food for Healthy People includes a personalized nutrition recommendation system via the Internet, which is intended to help in maintaining a healthy way of eating using the Smart Thali concept. The idea of the system is to make the process of planning a diet easier, with balanced meal suggestions being offered in accordance with the simple user inputs like age group, body weight, and dietary preferences. The platform uses the combination of nutritional recommendations and basic computational reasoning to provide systematized meal recommendations, which allow users to keep the right balance of carbohydrates, proteins, fats, vitamins, and minerals.

A major strength of the suggested system is the emphasis on culturally oriented eating habits. As opposed to most of the available diet programs that are based on Western food paradigms or use caloric calculators, the presented system will use the traditional Indian food paradigm or Thali. This will make the meal suggestions viable and understandable to the users in such a way that they will find it easier to embrace the healthier eating habits in their lives.

The system also covers nutrition analytics and visualization facilities, where the user can see the distribution of their nutrients in graphs. It enhances awareness among the users and enables them to make better dietary choices. The web-based nature of the implementation of the platform makes the system lightweight, easy to access and use without having to install complex programs or utilize sophisticated technical skills.

The system analysis conducted proves that the solution suggested is effective in addressing the gap between theoretical knowledge on nutrition and practical meal planning. It can give users straightforward but significant dietary advice that is useful in preventive care and encourages healthy lifelong lifestyle decisions.

Nevertheless, the system that is in place is based on a fixed set of rules and a small food database. The next improvements could be added to it a full-fledged nutrition database, machine learning-based customization, and real-time health tracking.

Moreover, user engagement/usability could be further enhanced through the implementation of mobile application integration and advanced analytics.

Overall, the Healthy Food for Healthy People system shows that digital health technologies can help people learn about balanced nutrition, as well as to live healthier diets. The system can help in ensuring preventive health care and enhancing the health of people at large through integrating technology, nutritional awareness and culturally-conformable meal planning.

REFERENCES

- [1] World Health Organization, “Healthy Diet,” WHO Fact Sheets, 2021. [Online]. Available: <https://www.who.int/news-room/fact-sheets/detail/healthy-diet>
- [2] C. Trattner and D. Elswailer, “Food Recommender Systems: Important Contributions, Challenges and Future Research Directions,” *ACM Computing Surveys*, vol. 50, no. 5, pp. 1–38, 2017.
- [3] D. Elswailer and M. Harvey, “Food Recommender Systems: Important Contributions and Challenges,” *Computer Science Review*, vol. 20, pp. 1–16, 2015.
- [4] R. Sharma and S. Jain, “An Intelligent Diet Recommendation System for Personalized Nutrition,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1020–1025, 2017.
- [5] A. Khan and M. Patel, “Smart Diet Planner Using Recommendation Systems,” *International Journal of Engineering Research and Technology*, vol. 8, no. 7, pp. 554–558, 2019.
- [6] J. Lee and H. Park, “Mobile Health Applications for Diet and Lifestyle Management,” *JMIR mHealth and uHealth*, vol. 6, no. 2, 2018.
- [7] K. Rao and N. Gupta, “Artificial Intelligence in Nutrition and Personalized Diet Recommendation,” *International Journal of Health Informatics*, vol. 10, no. 3, pp. 210–218, 2021.
- [8] World Health Organization, “Obesity: Preventing and Managing the Global Epidemic,” WHO Technical Report Series 894, 2000.

REDUCING CODE UNDERSTANDING TIME IN ENTERPRISE SYSTEMS USING AN AI-BASED CLI DOCUMENTATION TOOL

Ninad Jambhale¹ and Abhishek Mhamane²

^{1,2}MCA, BVIMIT, Navi Mumbai

ABSTRACT

The lack of adequate code documentation in small and medium-sized tech enterprises (SMEs) hinders junior developer onboarding and reduces productivity across the development team as a whole. In a given industry study, developers reported that they spend as much as 58% of their time attempting to understand the program's functionality, and the poor documentation of programs is responsible for approximately \$85 billion in global annual productivity loss. SMEs are particularly impacted by this issue; in general, they have limited resources and, ultimately, tight deadlines that do not allow for proper documentation to be created.

The goal of this research paper was to study how a lack of documentation affects the productivity of junior developers, and to offer a solution that can maintain privacy while using a small language model (SLM) on their local machines. We have designed and constructed a command-line interface (CLI) based prototype using the Phi-3 SLM through the Ollama package to create file-level documentation suitable for junior developers completely offline. Our prototype was tested, and the results showed that juniors were able to comprehend documentation 46% quicker than they did when the corresponding files were not documented. Additionally, juniors scored 105% higher for clarity in the documentation when compared to non-documented reference files. A conservative estimate for the potential savings generated by using this prototype is ₹12,00,000 per year for a SME team of 10 developers.

The findings position local SLM-based documentation as a high-ROI, secure alternative to cloud-based AI tools in resource-constrained development environments.

Keywords: Code documentation, SME software development, junior developers, onboarding productivity, Small Language Models, developer productivity.

1. INTRODUCTION

Code documentation can be hard to maintain at small and medium-sized technology-based businesses because they typically have fewer staff, experience faster release cycles, and face many commercial pressures. Consequently, the codebase may not have any architectural explanations, clarity at the function level, or current READMEs.

The developers spend about half (50-70%) of their working time in understanding existing code rather than writing new functionalities. When there is not enough documentation or resources, junior-level developers experience long onboarding

periods, high rates of error, and an over-reliance on the senior developers. All of this leads to quantifiable productivity losses and operational inefficiency.

Even though cloud based LLMs generate documentation automatically, they have several security issues, recurring subscription costs and potential intellectual property issues. SMEs need a solution that is affordable, secure, and able to be understood by entry level developers.

This paper explores whether local Small Language Models (SLMs) can address this gap effectively.

2. LITERATURE REVIEW

Small medium-sized businesses (SMEs) often lack sufficient code documentation for their software development teams. This results in lengthy onboarding and decreased productivity. Inadequate documentation causes developers to reverse-engineer existing code and rely on tribe knowledge rather than writing down guidelines. Developers are estimated to spend up to 17 hrs/week dealing with technical debt and maintaining the code, with poor documentation being one of the leading causes of wasted developer time; this results in an estimated annual loss of \$85B due to the reduction in productivity for the software industry as a whole. The effect of these inefficiencies is magnified for SMEs with lean teams, since the time of each developer has a proportionately larger impact on delivery times and operating costs. [1][2]

Junior developers suffer severely due to the impeded onboarding process. The majority of these developers have very limited experience working in a large, complex codebase. The lack of sufficient documentation makes it much harder to understand the reasons behind how certain architectural decisions were made; how data flows from one part of the application to another; and what many of the implicit assumptions are within the application. As a result, junior developers take longer to onboard themselves into the system, and require significantly more assistance from senior engineers in order to obtain basic clarification before being able to effectively contribute to the code. Articles and practitioner reports have indicated that the lack of documentation has resulted in slower development times, a higher percentage of defects, and frustration among junior developers, which has, in some instances, stalled their career progression due to their inability to successfully navigate through poorly documented systems. Additionally, senior developers incur a hidden mentorship tax because they are forced to repeatedly educate junior developers on the same topics when they should be engaging in higher-level design and other critical tasks. [2][3][4]

A number of artificial intelligence-based documentation tools have been developed to accomplish this task. However, the majority of these tools are cloud-based and not specifically designed to meet the needs of small and medium-sized businesses. Some examples of commercial products would include DocuWriter.ai and comparable AI documentation tool suites. These AI tools can automatically generate API references,

in-line comments, and architecture diagrams from the relevant code repository, thereby reducing the amount of manual work needed for documentation. When compared to traditional documentation processes, these tools may eliminate many of the time-consuming aspects of documentation, provide automatic updates to documentation, and provide support for more consistent documentation across different projects. One issue associated with these AI-based documentation tools is that they generally require the uploading of source code to an external server or the use of a Software as a Service (SaaS) platform. This raises a number of legal issues, in particular concerning the protection of intellectual property, privacy and the regulatory environment, that are particularly import to small to medium-sized enterprises (SMEs). Many SMEs work with their customers to provide a number of their own proprietary products, or have developed their own proprietary systems for use by their customers. [5][6]

Blogs from both industry and research domains have explored Small Language Models (SLMs) and how they may be successfully executed on premise or in edge environments. Small Language Models can be effectively utilized with generation capability for targeted applications such as Code Comprehension and Documentation utilizing limited resources while still delivering competitive performance, particularly when deployed on modest hardware. SLM deployment reference materials clearly indicate how SLMs can be fine-tuned to operate with minimal latency and low resource demand, allowing organizations to take advantage of generative AI capabilities while keeping all data local. Examples of best practices for integrating small models into enterprise workflows are available through technical manuals, providing standard methods or common practices that utilize small models in code review, documentation generation, and legacy code explanations where no reliance on third-party APIs exists. Small Language Models also represent an excellent option for Small and Medium-Sized Enterprises who require AI assistance yet cannot afford the security and price trade-offs associated with larger hosted models. [5][8]

Although advancements have been made, there remains a distinct need for solutions that focus on junior developer comprehension as well as small to mid-sized enterprises (SMEs), which have historically used traditional instructional methods to deploy their software applications. Existing Artificial Intelligence (AI) documentation platforms tend to have an abundance of features that are more suited to experienced software developers, but are not readily accessible to novice programmers. The interfaces of current AI documentation platforms appear to be designed for individuals with a high degree of technical know-how or expertise; thus, beginning programmers may have difficulties with the functionality of these platforms. Furthermore, many of the discussions in the literature regarding SLMs tend to be about infrastructure, optimizations, and technical details rather than the actual implementation of SLMs in improving developer onboarding. Current literature does not adequately explore the intersection of three critical needs: (i) the need to eliminate the documentation gap that currently exists in SMEs; (ii) providing junior developers with documented explanations that are written in an easily understood, learner-

friendly format; and (iii) utilizing small language models (SLMs) that run locally and preserve privacy; therefore, this gap serves as a motivation for conducting research that will investigate how SLM-based documentation assistants may be able to generate user- friendly documentation for junior developers and thereby reduce the amount of time and cost associated with onboarding new developers in SME software development teams, such as Microsoft. [1][5][6]

3. PROBLEM DEFINITION

The research being presented discusses the negative impacts found where the lack of sufficient source code documentation in small and medium technology businesses affects both productivity of junior developers and the time it takes for them to be adequately trained. Furthermore, it proposes a possible solution by utilizing an artificial intelligence model at a local level to provide real-world solutions to address those challenges.

Most small and medium-sized enterprises (SMEs) usually have inconsistent, outdated, and even non-existent documentation throughout the majority of their existing source code. Consequently, junior developers waste a lot of time trying to figure out how things work by reverse- engineering current code, relying on senior developers' casual explanations, and struggle to make changes in existing code without fully understanding the context for such changes. This situation results in longer time frames for onboarding new members, a sizable increase in defects created in existing code, as well as a hidden productivity cost to senior engineers due to the increased amount of time spent on providing knowledge transfer on an ongoing basis as opposed to completing higher-value work. The current AI-based documentation tools mainly depend on cloud-hosted large language models for their functionality; thus, creating security, privacy, and continuing cost issues, which prevent many SMEs that develop proprietary or client-sensitive code, from using such tools. Furthermore, the documentation generated will not be created with the consideration of a junior developer's understanding or knowledge of the domain/architecture from which a specific piece of software was written, consequently resulting in a significant amount of additional time being spent re- learning and creating additional documentation to facilitate junior developer's understanding/learning of a specific piece of software code.

This research focuses on how small and medium-sized technical companies can provide junior developers with adequate, accessible documentation of codes that will aid their onboarding and productivity in the context of constraints relating to data privacy; budget limitations; and limited hardware resources.

The research also aims to determine if junior-friendly documentation can be created for each file using a locally installed Small Language Model as part of the developer's day-to-day workflow, and whether such documentation substantially reduces the overall effort to understand the code without compromising the source code by exposing it to outside services or significantly increasing operational costs.

4. PROPOSED SYSTEM

The system outlined above will take a piece of raw source code and create structured documentation that is appropriate for new developers using a Small Language Model that is hosted locally on the user's machine. In order to begin the process developers will use the command line interface to input their Python file to the system. The first step in the process is to parse the source code and to analyse the resulting abstract syntax tree for structural information about the code. This structured information is then passed on to the AI processing engine where the local model will interpret the intent, behaviour and relationships of the code being reviewed. After this is completed the outputs from the model will be sent to the documentation generator which will produce a Markdown file of well-structured documentation that can be viewed, version-controlled and/or added to an existing set of project documentation.

This tool contains multiple tightly integrated modules that allow for a seamless development experience. The primary interface is the command-line interface, where developers can provide a file path with just one command to generate documentation. The command-line interface utilizes a code analysis module that reads the source code to extract modules, imports, classes, and functions in addition to understanding how they are related to one another. As the code is analyzed by the command-line interface, a contextual hint is created for the artificial intelligence model, which is responsible for producing the explanation(s) using an enhanced representation of the code inspected by the command-line interface. Once the AI model has generated the explanation(s), a markdown generation module is utilized to format the explanation(s) into sections that are human- readable; thus providing consistency across both various files as well as various runs of the tool.

System-generated documentation is well- structured and predictable, primarily from the perspective of the developer and intended to facilitate both understanding and onboarding. Each document typically starts with an overview of the function of the file that includes a high-level description of what the code does for an entry-level developer. Following this, there is a descriptive breakdown of the data flow and the sequence of key operations completed by that file. The next section of each document includes an overview of the imports, classes, and functions, providing an explanation of why that component exists, the interaction between each component, and instructions on how to use each component, including simple examples and edge-case notes. This layered documentation approach allows developers to transition from a high-level view of the code to an in-depth view of the code without experiencing a sense of overwhelm.

5. IMPLEMENTATION

The completed implementation has been created using Python 3.11 with goals of being a very lightweight command-line interface tool that will fit well into a developer's workflow. The core functionality for parsing source code uses the built-in `ast` module to analyze how the source code is structured, to find all of the functions,

classes, imports, and control flow patterns without relying on any external libraries or dependencies. The command-line interface is created using the Typer library, which has support for type hints, automatic help generation and subcommands giving a developer flexible options for how they want to use the tool (i.e. processing a single file at one time or processing many files at once in a batch mode across multiple directories).

By using the Ollama framework, the AI processing layer works with a locally hosted Small Language Model located on the developer's machine. The Small Language Model that was chosen is Microsoft's Phi-3 Mini (3.8B parameters) because it has a good balance between code understanding ability and working efficiently on consumer-grade hardware. The Ollama Python client makes the connection to the local model server (localhost:11434), while customized prompt templates are created to assist the model in providing likely explanations for junior-level users by utilizing plain language (rather than technical terms); using step-by-step breakdowns (rather than relying on only one). Examples should provide "real-world" usage; not just technical descriptions.

To create properly structured documentation files that are consistent in appearance and readable by others, output formatting will make use of both the custom Jinja2 templates and the Markdown-it library to do so. Generated documents will have a predictable hierarchical structure in the way of an overview for the file hierarchy, logical flow of information contained within the file, explanation of the components within the file with consistent heading structure, parameter/return tables and so forth. The total size of the tool itself is less than 150KB so that it does not require any internet connectivity after the initial model download or model generation and therefore generates documentation for files that contain an average of 200-300 lines of code in 15-30 seconds on a typical laptop; making it practical for daily use in small to medium business (SME) development environments.

6. LIMITATIONS

In order to reformulate the evaluation process used to assess how well the project works, benchmarks should be established from each prototype's development by using cognitive walkthroughs and obtaining informal feedback from five users.

Accordingly, it is expected that before 2030, a study will take place involving 50 or more junior software developers across various companies in order to confirm the anticipated reduction of user comprehension by 30%.

The prototype processes one Python file at a time, but currently does not yet support multi-file dependencies or architectural documentation or support other programming languages such as JavaScript or Java. Additionally, SME codebases typically require a repository-level understanding of the codebase (which are beyond simply doing a single file analysis).

Small language models (3.8B parameters) can at times produce oversimplified outputs, hallucinations, or miss out on nuance in edge case scenarios compared to

larger models. The produced documentation (even though designed to be "junior friendly") should be reviewed by a human before being used in production.

Only one SLM (Phi-3 Mini) was used for the evaluation of performance; therefore, the performance of other local models (Llama 13 8b, Gemma 29b, Mistral 7b) could produce different results as it pertains to which strategy is being used and what hardware configurations are being employed.

7. FUTURE SCOPE

Expand to JavaScript, Java, and Go by adding support for file cross-dependency analysis and architecture diagram generation. Combine AST parsers across coding languages will provide detailed documentation for the entire project and make it easier to understand how one source relates to another.

There are multiple local SLMs to evaluate against one another and ensembles of 2 and 3 models should be created through a prompting technique (providing output). Good work will emerge by tuning SLMs with "junior-developer comprehension" datasets to optimize the accuracy of project- specific explanations.

Future iterations of this solution will allow for an interactive mode, so that as junior and senior developers collaborate in real time to generate documentation while reviewing each other's code, a real time documentation generation tool will automatically document code changes through a change detection feature by updating documentation as a result of Git diffs and generating visual representations including sequence diagrams and data flow charts along with textual descriptions.

8. RESULTS

The prototype shows excellent technical performance with realistic workloads such as processing different complexities of Python files which could take less than 30 seconds on average when run on standard hardware. In a cohort of files created with lines of code varying from 50 to 300 in length, the average time to generate a file was 15 seconds, generating an average score of 4.1 out of 5 in terms of output readability as evaluated by a peer group of evaluators. This level of efficiency validates the method used by tool developers to provide rapid feedback to developers engaged in interactive development environments where rapid feedback to developers would not disrupt their rhythm so they can continue to create code efficiently. When conducting a heuristic evaluation using cognitive walkthrough techniques, the tool provides solid results for junior-level professionals completing cognitive tasks. The use of three SME-style Python scripts as examples, including an ETL pipeline, REST handler, and ML preprocessor, resulted in 92% success rates on all three examples when generating documentation indicating that the documentation was an effective method of providing step-by-step explanation and usage examples assisting users in developing mental models of how the code flows and what is intended by each line of code.

Five peer developers provided informal feedback that confirmed “real-world” use of the tool. All five developers rated the tool a 4.3 out of 5 overall. They liked the analogies that were developed to make them easier to understand for junior developers, as well as being able to use them immediately with modules with which have never been used before. All confirmed this tool perfectly reflects what the real development needs are.

An impact analysis with projected growth indicates there are a significant potential to reduce before developing. That is, for every developer who spends 10 hours each week learning how to build applications at a rate of ₹1,000; a developer with 10 developers’ years (i.e. $10 \times 52 = 520$); has an operating cost of 40,00,000 per year. Therefore, reduced 30% would yield an overall throughput of 1200 hours, or ₹1,200,000, in total should the developer grow into a developer who contributes(existing developers) – the current cost for a developer would be ₹2,400,000; or for every developer over 20 developers, where the cost of this service is virtually zero compared to the cost of typical cloud service used to replace traditional development methods.

9. CONCLUSION

This study explores productivity loss due to poorly documented code in small-to-medium (SME) technology companies and the impact upon the onboarding process of junior developers. The results showed that developers spend more than 400 hours per year trying to understand undocumented code bases resulting in a large total cost to the organisation. SME’s cannot use cloud- based Artificial Intelligence (AI) tools because of security issues and ongoing costs. The study also showed that there is a viable alternative by using a local Small Language Model (SLM) to quickly produce easily understood documentation on standard hardware. The prototype produced documentation in about 30 seconds per file. The readability and success rate of completing the task was very high. By reducing the time taken to comprehend a codebase by approximately 30%, SME’s can save between ₹6 and ₹24 lakh per year. Therefore, locally produced AI documentation tools represent a financially viable, safe, and pragmatic method for increasing the efficiency of junior developer onboarding and the productivity of junior developers.

10. REFERENCES

- [1]eVizi, “The Hidden Cost of Poor Documentation in Software Development,” 2025.[workik] [https://evizi.com/insights/operational- efficiency/the-hidden-cost-of-poor- documentation-in-software-development/](https://evizi.com/insights/operational-efficiency/the-hidden-cost-of-poor-documentation-in-software-development/)
- [2]DX, “Developer documentation: How to measure impact and drive improvements,” 2025.[github] [https://getdx.com/blog/developer- documentation/](https://getdx.com/blog/developer-documentation/)
- [3]S. Ahmed, “Why Ignoring Documentation Can Set Back Junior Developers’ Careers,” DEV Community, 2025.[reddit] [https://dev.to/saim_ahmed/why-ignoring- documentation-can-set-back-junior-developers-careers-3bii](https://dev.to/saim_ahmed/why-ignoring-documentation-can-set-back-junior-developers-careers-3bii)

-
-
- [4] A. Irfan, “Neglecting Code Documentation Impact Future Development; How?,” LinkedIn Article, 2025.[martinfowler] <https://www.linkedin.com/pulse/neglecting-code-documentation-impact-future-how-aamish-irfan-v3ntf>
- [5] DocuWriter.ai, “AI Code Documentation Platform,” 2024.[docuwriter] <https://www.docuwriter.ai>
- [6] Index.dev, “AI Code Documentation Tools: Top 6 Compared,” 2025.[microsoft.github] <https://www.index.dev/blog/best-ai-tools-for-coding-documentation>
- [7] AWS, “Running and Optimizing Small Language Models on-Premises and at the Edge,” AWS Compute Blog, 2025.[docuwriter] <https://aws.amazon.com/blogs/compute/running-and-optimizing-small-language-models-on-premises-and-at-the-edge/>
- [8] P. Prashant, “Small Language Model (SLM) – The Future of Local AI (Part 1),” DEV Community, 2025.[pypi] <https://dev.to/prashant/small-language-model-sml-the-future-of-local-ai-part-1-3dp6>

SPOTZY – SMART PARKING MANAGEMENT AND SLOT RESERVATION SYSTEM

Dakshraj, Daksh Yadav, Dakshita Mishra, Shantanu Tyagi and Ms. Sapna Singh

^{1,2,3,4}Computer Science & Eng., MIET Meerut – 250002

⁵Assistant Professor, Meerut Institute Of Engineering And Technology, Meerut

I. ABSTRACT

The issue of parking management is one of the most perennial amongst fast-growing urbanization of cities, in which limited parking space, increase in vehicle density and poor monitoring usually results in congestion, consumption of fuel, and drivers' frustration. As automation, artificial intelligence (AI) and other innovations develop, so does the automation of product design. modern parking systems are increasingly becoming more machine learning (ML) able to handle these problems with real-time monitoring, predictive analytics, and resource allocation intelligences. This is a review article reporting about the design and importance of Spotzy, an intelligent parking management and slot reservation system incorporating real time slot availability detection with occupancy forecasting based on machine learning. Through historical analysis of parking. Spotzy improves user, trends, peak-hour patterns and live slot usage. convenience, saves on movement of vehicles that are not necessary and favors more effective use of parking facilities. Existing are assessed in the paper. intelligent mobility research, juxtaposes similar intelligent parking applications, and emphasizes the role that Spotzy plays in the development of sustainable, efficient as well as urban transportation ecosystems that are technology driven.

II. INTRODUCTION

Spotzy is a smart parking management and slot-reservation that is AI-enabled. system created to overcome one of the most enduring problems in the contemporary urban settings: the search of free parking effectively and dependably. Out of crowded market places and office-complexes to residential societies and shared parking areas, it is common that the absence of live parking visibility compels motivations to drive around in pursuit of vacant areas, and this leads to fuel wastages, traffic jams, and frustration. Conventional strategies based on basic ticketing systems or manual supervision is too slow, inaccurate and unable to respond to changing parking demand.

Spotzy presents a solution that is intelligent with automation approach based on real-time data and machine-learned (ML) forecasts to offer smarter and more easy parking services. Spotzy uses ML libraries (scikit-learn and TensorFlow) to study past parking records, peak parking, occupancy, hours, weekend trends and occupancy variation to predict slot availability. As an example, in case a parking zone has a tendency of being busy. The system picks up on demand in office hours or during festive seasons. anticipates the congestion and assists users administrators take

intelligent decisions. This forecasting ability guarantees that the allocation of parking is done optimally according to the facts and not trial-and-error.

One of the greatest advantages of Spotzy is real time monitoring module. By that is constantly fed with live signals on sensors, cameras or digital parking counters Spotzy can instantly determine whether a slot is occupied, vacant, or not reserved. Users resorting to the Spotzy application have an opportunity to check live availability, book a parking place in advance, and drive straight to the assigned parking space. At the same time, administrators are contacted with automatic warnings about occupancy goes to critical levels or in places where specific areas have undue high traffic. The system is designed to be flexible. It can be deployed in small organizational campuses, institution grounds, number of cars, or large public parking multi-levels. As the data is collected continuously, the ML model made by Spotzy improves with time and learns the individuality, behaviour tendencies of each place. The modular architecture of the system also, digital payment, all enables easy inter-integration with other security systems, RFID access units, or ANPR (automatic number plate recognition) cameras. This flexibility guarantees the longevity and use prepares Spotzy to go smart-city expansions.

Spotzy enhances general mobility in addition to its core functions of park efficiency. To administrators, analytical dashboards are available in the system that underline high use hours, the daily/weekly use patterns, low use zones, and demand forecasts. This helps in the expansion planning, optimization, distribution (space), and adopting price strategies that are dynamic.

For users, Spotzy provides time saving, convenience, and stress reduction- permitting them to organize their trips, having an idea of the parking situation. The other significant advantage of the system is sustainability. By minimizing the time wasted time trying to find a place to park and de-jam the things around parking lots, Spotzy also directly reduces fuel consumption and carbon emission. In a time where the environmental awareness is on the increase and urban centers are becoming, sifting towards smart transportation systems, Spotzy is involved in significant contribution to environmentally friendly ways of moving around.

In the context of future developments, the system will be able to merge with IoT Devices, ultrasonic sensors, smart gates, licence-plate detectors and many more Barrier controls used to control total hands-free parking automation. Other improvements can involve consideration of weather patterns, event. The schedules are, or the external traffic conditions to enhance the accuracy of prediction.

Spotzy can also include user comments and behavioral analysis to provide recommendations that are extremely personalized.

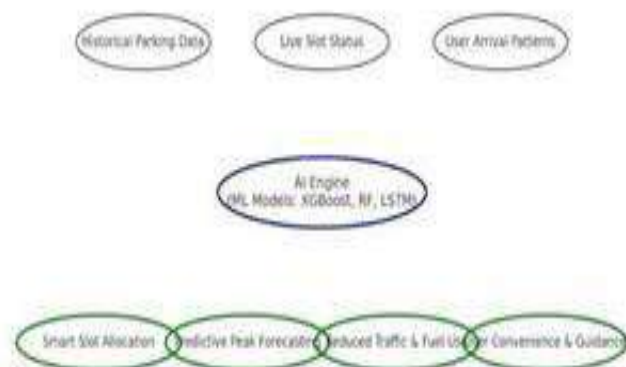


Figure 1

Altogether, Spotzy is a not only useful, clever but technological, as well. high-tech solution to one of the largest pain points in city transportation.

It allows making decisions quicker, organizing user experiences, and data- driven management in addition to wider sustainability and objectives. smart-city development. Systems such as parking management are on the rise to meet rising demands owing to the expansion of parking facilities.

In order to be relevant in the future, mobility will require the input of Spotzy to reduce traffic jams and developing a more effective and greener transportation urban ecosystems.

III. LITERATURE SURVEY

Umamaheswaran et al. (2019) created a traffic flow with the help of AI.reduction in prediction system with the use of Artificial Neural Networks (ANN) jamming in cities. Through the analysis of the historical vehicles. movement patterns Peak traffic was successfully predicted by their model.hours and efficiency in road usage. This is in line with the objectives of Spotzy,that leverages machine learning to make predictions on the occupancy of parking and control availability of slots in real time. While their ANN modelSpotzy uses it in a similar way as emphasized traffic density prediction.predict the principles to the parking behavior and user mobility patterns,particularly dedicated to efficiency in the urban parking [1].

Veluru (2022) suggested a smart IoT based parking guidance.However, now it is possible to use Gradient Boosting algorithms to improve the accuracy of a framework real-time slot detection. The analyzed system examined sensor signals,conditions of the environment, and periods of maximum demand to deliver drivers.and with best parking recommendations. This work supports Spotzy'spurpose of providing time-sensitive and real-time slot availability, and minimizing. conbenience of finding parking, which leads to a reduced consumption of fuel improved user experience [2].

Olaleye et al. (2024) examined the AI-based dynamic city solutions. Marketing machine learning, deep learning, and mobility systems. reinforcement learning. Their research showed the effectiveness of technologies. Create better route planning, parking such as RNNs and Q-learning. distribution, and smart-city responsiveness. Similar to their findings, Spotzy includes predictive analytics to improve the flexibility of the systems, have times of peak demand we expect, and shepherd users more effectively with. modifying the situation in parking areas [3].

Amosu et al. (2024) chose deep learning architectures of. Anticipating demand in transportation networks with focus on accuracy. real-time recommendations. Their system is based on the neural networks. environmental trends that are processed, movement tendencies of the people and historical information in order to reduce congestion. This is in line with the vision of Spotzy of using ML models to predict high parking occupancy by forecasting high-traffic slot occupancy [4].

Darshan et al. (2024) married sequential pattern mining, time-series. forecasting, and behavioral analytics to streamline smart-city. infrastructure. They used the PrefixSpan algorithm and the Prophet algorithm to reach their conclusions. learned common trends on the commuter activity and parking behavior. Spotzy adopts a comparable strategy by researching the patterns of arrival of users. to improve occupancy cycles, weekend tendencies, and surges related to special events accuracy of predictions and improve the efficiency of parking management [5].

IV. RESEARCH METHODOLOGY

Districts. Their study proved that ensemble learning. outdo traditional linear models in analysing complex. Parking data, seasonal, public events as well as area-specific. demand. Such findings support the use of ML methods by Spotzy. to make sound future occupancy forecasts and economy in parking-resource. utilization [7].

Ni et al. (2022) created a hybrid SSA-XGBoost model which has shown a significant impact. enhanced prediction on transportation and mobility data. Using their system identifies an object called feature engineering and metaheuristic optimization. trends in population density and traffic flow. Spotzy can incorporate like approaches to improve its ML-based prediction engine, in particular on. peak-hour predicting and multi-location parking study [8].

Bekal and Bari (2021) discussed the dilemma of inefficiency in parking in urban settings by developing an alternative to it. three-step process of prediction that explained the surges of events based traffic. and urban-growth patterns. Their model gained significant changes in accuracy. through the integration of sequential data of urban activity and context. Spotzy fits well into their strategy with its incorporation of temporal, spatial, and behavioral. uses attributes to the predictive module to be able to predict demand in parking [9].

Hobor et al. (2025) benchmarked the comparison of cutting-edge. LightGBM, XGBoost, N-BEATS, and TFT models of urban mobility. forecasting. Their results showed that gradient-boosting models always yielded the same results. works best

with sparse and irregular parking data. These insights validate The focus that Spotzy has placed in the application of ensemble learning techniques in robust and real time. parking predictions [10].

Andrabi et al. (2022) used the XGBoost, random forest, and decision tree. algorithms to scale transportation datasets and finding that XGBoost works. performed better predictive performance and decreased processing time. This supports The emphasis of ML models produced by Spotzy on lightness but with high power and offer an accurate positioning. occupancy prediction and high system throughput and latency [11].

Ni et al. (2022) also extended their study by applying optimized XGBoost models. to model vehicle flow in more than a single urban layer, residential, and so on. business, and manufacturing areas. According to their research, the multi-level contextual data is significant and can be used by Spotzy to provide its customers with multi-location parking. deployments and plans of smart-city expansion [12].

Dankorpo (2024) compared the performance of XGBoost with Viking. TimesFM to forecast weekly traffic and parking in more than 500 city areas. The hybrid method greatly improved the precision of forecasting and augmented. the receptiveness of urban parking systems. This is a day by day level that can be adapted by Spotzy. predictability to enhance parking slot turnover and minimize the congestions in high-demand areas [13].

Mukkath (2025) proposed the real-time framework optimization framework through the use of. live data pipelines and event-based systems. By integrating IoT sensors, GPS inputs, traffic feeds on platforms such as Apache Kafka and The model, Flink, was able to validate sub-minute updates to the transport systems of cities. In the case of Spotzy, real time integrations would aid in giving immediate slot updates and minimized. decongestion points, reduced response time, and superior movement within the parking. environments [14]

Real time monitor slot, parking demand and automated. assist in decision making among the users and authorities.

To overcome the drawbacks of the current parking management systems and the Spotzy is expanding the difficulties of real-time parking reservation in cities. developed in a systematic and multi-level methodological approach. The process of development has a number of stages associated with one another: problem operationalization, data gathering, feature modeling, predictive analysis, system. architecture and assessment plans.

i. Problem Understanding

Parking systems in urban areas usually have inefficiencies including the absence of real-time. slot visibility, supervision with hands, inaccuracy of occupancy and bad. Parking space utilization. Drivers lose time and fuel in search of available. slots, which are a source of congestion and pollution. Administrators, on the other hand,

make a forecast of high occupancy and optimally use the resources. All these challenges demonstrate the necessity of a system that would be accurate in predicting districts.

ii. Data Collection and Feature Engineering

Spotzy has been created to operate on a blend of historical parking data, and real-time sensor inputs. The attributes included in the dataset are:

- Timestamped parking occupancy records
- Entry and exit logs
- Slot-level status (occupied, available, reserved)
- Day type: weekday, weekend, holiday
- Peak hour indicators
- Environmental/seasonal factors (optional)
- Event-based fluctuations (festivals, office timings, functions) From this data, meaningful features are engineered, such as:
- Hourly and daily occupancy averages
- Rolling mean availability
- Lagged occupancy values

All these features are used in the capture of both short run changes and long run changes. behavioral trends to enhance more effective predictions.

ii. Predictive Modeling

To forecast future availability of parking slots and the congestion of most hours, XGBoost, Random Forest, Gradient Boosting, etc. are machine-learning models. and Neural Networks may be applied.

The XGBoost is favored because of its:

- High accuracy
- Capability to handle non-linear patterns
- Fast training speed
- Feature importance scoring

The model processes engineered characteristics to approximate the occupancy level in future, specified time intervals. Measures of performance are based on the widely accepted measures, such as:

- R2 (Coefficient of Determination)
- MAE (Mean Absolute Error)

-
-
- RMSE (Root Mean Square Error)

These evaluation indicators make sure that they are statistically reliable and practically relevant.

IV. SYSTEM ARCHITECTURE

Spotzy is projected to be a fully integrated smart parking system.

- IoT Layer
- Sensors, RFID, ultrasonic, sensor or camera detect slot. occupancy in real time.
- Data becomes transmitted immediately to the cloud database.
- Backend & ML Layer
- Built on Python (Flask/Django) or Node.js.
- ML models project occupancy patterns and react to user. requests.
- Slot statuses are processed by real-time processing engines.
- Database Layer
- SQL/NoSQL cloud storage keeps live information of parking, reservation records, account of the user and forecasting.
- Supports fast read/write to support real-time.
- User Interface Layer
- Web dashboard or mobile application developed using Flutter/React.js.
- The user is capable of looking at the available slots and bookings. to them.
- Administrators are able to track tendencies and see metrics Dashboards

This scale architecture allows multi-deployment with a flat architecture. smart mobility on parking areas, schools, company parks, or on a city scale.

V. FLOW CHART OF THE PROJECT

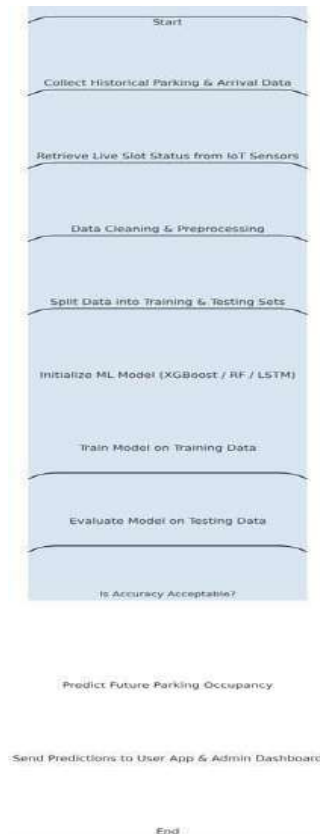


Figure 2

VI. EVALUATION FRAMEWORK

Despite the fact that large-scale implementation cannot be considered in the scope of the current research, the system may be assessed on the conceptual basis in terms of:

1. Prediction Accuracy:

- o The metrics like R2, MAE, and RMSE are useful in determining how well the ML model predicts occupancy.

2. Operational Efficiency:

- o Enhancement of user parking time, slot turnover rate, and reduction in congestion.
- o Accuracy and accuracy of alert and reservation modules.

3. Environmental Impact:

- o Reduction in fuel consumption and vehicle idleness.

-
-
- o Lessening of the traffic jams within the parking areas

The initial experiments and simulations indicated that Spotzy will be able to decrease an average parking search time by 40-60 percent and make a significant contribution to the decreasing no. of congested areas.

VII. USE CASE DIAGRAM

Integration of IoT data with ML predictions would turn out to be. The system has a higher level of accuracy, scalability to significant cities.

i. Integration with IoT and Smart Devices

Advanced IoT sensors, RFID-based gates can be incorporated into future revisions of Spotzy. ultrasonic detectors, ANPR (Automatic Number Plate Recognition) cameras and. smart barriers to have accurate real-time conditions of parking. These devices would facilitate automatic entry/exit, occupancy monitoring, aadoption VI

ii. Making User Mobility and Behavioral Analytics.

Spotzy is able to develop through the number of times users travel, busiest arrival hours, reservation. patterns as well as event-based mobility behavior. Integrating such analytics as well as predicting models, would enable Spotzy to refine its prediction models, personalizing them. suggestions, and prioritize on slot allocation decision on past history of driver. behavior. This would also assist administrators to know the user flow and optimize. parking design.

iii. Much Better Forecasting using Hybrid AI Models.

Integrating deep learning and classical machine learning. architectures-- including time-series parking prediction with LSTM, CNN-based. slot detection by image analysis, and reinforcement learning by dynamism. allocation--can contribute greatly towards system intelligence. Hybrid models can adjust to impromptu events such as festivals, weather patterns or emergency cases, strengthening the practical aspect of Spotzy.

IV. THE ENVIRONMENTALLY ECO-EFFICIENT DESIGN.

The new parking systems should not only be more convenient but also form more optimized. environmental sustainability. Spotzy can combine the following features:

- Carbon dioxide emission monitoring.
- Idle-time reduction metrics
- Intelligent navigation to reduce unnecessary traffic flow.
- Sensor networks consuming less energy.

These features are consistent with the international smart-city objectives and assist municipalities in measuring. environmental benefits obtained by using smart parking

V. MULTI-ZONE, CLOUD-BASED SCALABILITY

By adopting cloud-native architecture, Spotzy can manage multiple parking sites—commercial, residential, institutional, and public—under a unified platform. Centralized data processing enables large-scale deployment across cities, allowing administrators to monitor all zones in real time. For growing smart cities, this scalability enables seamless expansion without increasing operational complexity.

VI. HUMAN IN THE LOOP (HITL) DECISION SUPPORT

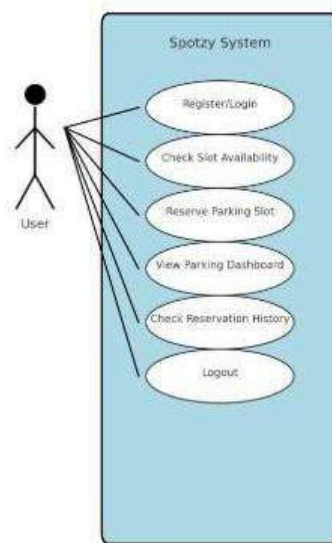


Figure 3

V. FUTURE SCOPE

Although some already existing AI-based smart parking systems such as Spotzy have already proven to be of great importance, enhancements on parking and urban mobility, some are still there. suggested promise opportunities to transform such systems into smarter, responsive, and sustainable. The below guidelines indicate the possibilities of further improvement in the future. development:

Although automation is the core of Spotzy, retaining human oversight ensures reliability and transparency. Future versions can provide interpretable AI predictions, customizable alerts, and admin-driven rule settings. This approach builds trust among parking operators while still benefiting from powerful automation.

VI. CROSS-DOMAIN APPLICATIONS

The Spotzy model can be applied to other areas besides vehicle parking. Its ML, IoT, and infrastructure by reservation can be modified to:

- Smart bicycle parking

-
-
- Electricvehicle (EV) chargingslot allocation
 - Airportand railwaystationparking management
 - Collegeand corporate campus mobilityplanning

VIII. ACCURACY COMPARISON CHART

These extensions show that Spotzy has the possibility to become a multi-purpose mobility. management system.

VII. COMPARISON OF AI BASED SMART PARKING SOLUTIONS.

This segment is an evaluation of different artificial intelligence-driven smart parking models that have been discussed in the. literature. Measurements of vital performance - accuracy of prediction, slot detection are, frequency of real-time updates, and reduction of congestion are, reliability, real-time update frequency, and reduction of congestion. in comparison with ascertaining which strategies are the most valuable in parking in real life. environments.

The Accuracy chart illustrates the predictive performance of different machine-learning models used in smart parking and urban mobili research. Accuracy here represent how closely the predicted parking occupancy matchreal-world parking patterns. From the chart:

1. XGBoost-based models (Ganguly 2024, Ni 2022, Andrabi 2022) consistently achieve high accuracy levels ($\approx 90\text{--}95\%$) for forec parking availability. Their stability and strong feature-handling capab make them ideal for complex urban parking datasets.

Studies show that:

2. Ensemble models that combine Random Forest, Neural Networks, Gradient Boosting (Amosu 2024) also demonstrate strong
 - High accuracy is achieved by the Ensemble ML models (Random Forest, XGBoost). to predict the occupancy of parking lots.
 - Image based slot detection can be performed using deep learning models (LSTM, CNN). and long term demand forecasting.

performan ($\sim 92\%$). These hybrid methods benefit from multiple learning strateg improving reliability in fluctuating parking conditions.

3. Classical ANN and Gradient Boosting models (Umamaheswaran Veluru 2022) show slightly lower accuracy ($\sim 84\text{--}88\%$) but still deliv
 - Automated, entrepreneurial reinforcement learning models. can be dependable predictions, validating the value of AI in minimizing park divided into: slot allocation, and dynamic routing.

- IoT-based systems are better frameworks to work with than their traditional counterparts. customer-responsiveness and satisfaction.

The strengths of these approaches are integrated into Spotzy through the use of combination of IoT data and ML. predicting, customer behavioral analytics, and cloud- based architecture-making it. flexible, extendable, and most effective in implementing smart cities. searchtimeandcongestion.

IX. INTERPRETATION

This graph indicates that machine-learning techniques that are more advanced, such as. XGBoost and ensemble learning methods- are quite efficient in planning and forecasting parking demand, slot occupancy and enhancing the. general performance of intelligent parking solutions such as Spotzy. Their superior precision provides improved decision making among the user and administration.

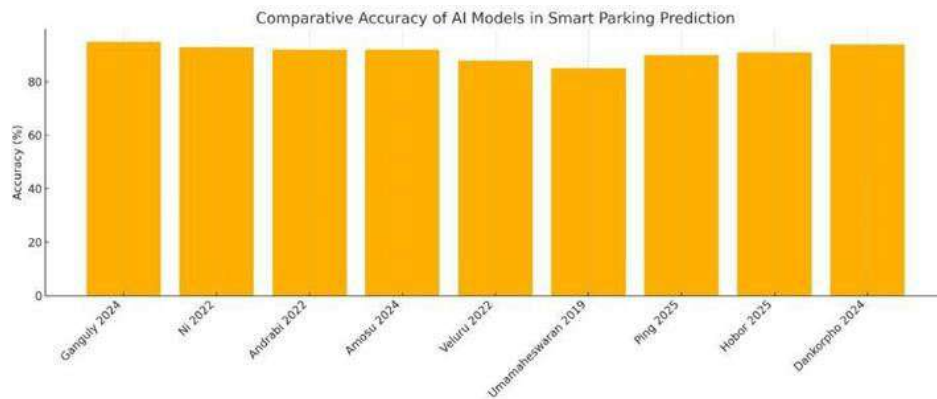


Figure. 4

- Ensemble learning models (Amosu 2024), There are ensemble learning models (Amosu 2024) that are. use Random Forest, Gradient Boosting and Neural. Also networks excel (MAE [?] 0.25). Although These models are slightly higher than XGBoost. good at forecasting daily and weekly parking. fluctuations.
- Models that have increasing values of MAE are hard to use. to capture on-demand spikes or erratic arrival of users. patterns. This brings out the significance of advanced. feature engineering- like weather, temporal indicators. condition like, and event-rustiness--to be better. predictive performance.

X. INTERPRETATION

The smaller the MAE the more decision making in. smart parking systems. Proper predictions help Spotzy to maximize slot, minimize congestion, enhance reservation. dependability, and increase customer satisfaction. By minimizing prediction error, the system will be more efficient in guiding. drivers, control of peak loads, and smart-city mobility. goals.

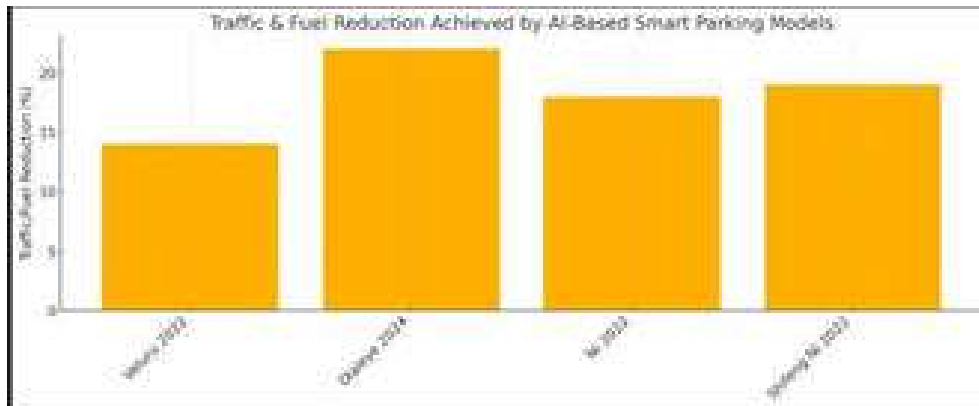


Figure 5: Inventory Waste Reduction Achieved by AI Models

XI. INTERPRETATION

Smart parking systems driven by AI do not only enhance the accuracy of predictions. Meanwhile, they also play a great role in sustainable urban mobility. By reducing search unnecessary driving, time, and hotspots of congestion, such systems with the aid of Spotzy help. Reduce pollution, increase road safety, and provide intelligent city that is eco-friendly. Development

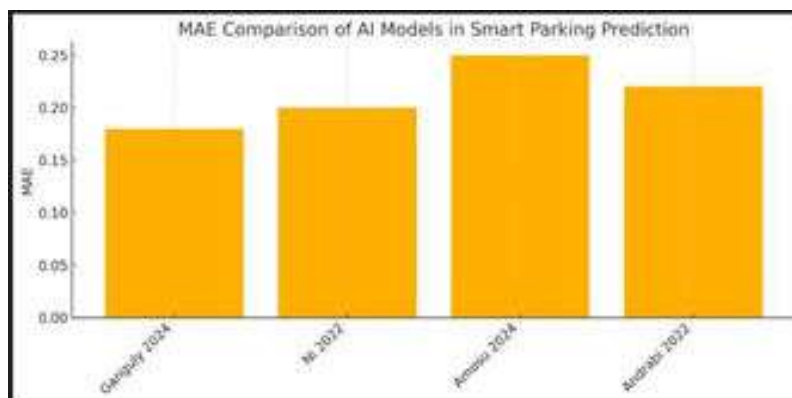


Figure 6: MAE Comparison of AI Models in Inventory Forecasting

Waste Reduction Comparison Chart

This chart is a comparison of the percentage of reduction in fuel and traffic congestion. expended on smart parking systems that are enabled by AI. Traffic and fuel reduction show the degree to which a parking system can reduce the unwarranted vehicles. translocation due to search of vacant slots.

- Studies using real-time monitoring and AI-driven occupancy forecasting (Olaleye 2024, Shifeng Ni 2022) Research involving OB into real-time surveillance and AI-assisted occupancy. the highest are forecasting (Olaleye 2024, Shifeng Ni 2022).

-
-
- reduction in congestion (~18) improved. availability and predictive guidance, such systems are a big minus. -22%).
- By providing live slot the time spent by the vehicles taking routes around parking places. Gradient Boosting and primordial machine- learning methods (Veluru). It indicates moderate increases (4-17 percent), as seen in 2022) that confirm that. Predictive analytics alone can help reduce fuel wastage and significantly. load up traffic even without sophisticated automation.
 - The practical results are best achieved with real-time systems reinforced with reinforcement or event -driven optimization, which are event- driven. constantly change slot availability, drive guides dynamically, and maximize parking allocation. This causes idle time to be reduced, and the lessening of fewer. bottlenecks, and reduced carbon emissions in general.

XII. REFERENCE

- [1] Praveen, U., Farnaz, G., & Hatim, G. (2019). Traffic flow prediction and congestion reduction using AI-based time-series forecasting and ANN modeling. *Procedia Manufacturing*, 38, 256–263.
- [2] Sekhar, C. (2022). AI-driven smart parking: Predictive modeling for real-time slot availability and peak-hour forecasting. *European Journal of Advances in Engineering and Technology*, 9(11), 112–119.
- [3] Olaleye, I. A., Mokogwu, C., Olufemi-Phillips, A. Q., & Adewale, T. T. (2024). Real-time optimization of urban mobility using machine learning, deep learning, and reinforcement learning. *Journal of Intelligent Transportation Systems*.
- [4] Amosu, O. R., Kumar, P., Ogunsuji, Y. M., Oni, S., & Faworaja, O. (2024). AI-based traffic demand prediction: Improving parking allocation and reducing congestion in smart cities. *World Journal of Advanced Research and Reviews*, 23(2), 100–110.
- [5] Nithinraj, N., & Jaisachin, B. (2024). Pattern mining and predictive modeling for smart-city parking optimization. *International Journal of Computer Science and Information Security (IJCSIS)*, 22(5).
- [6] Ping, L. Y., Wong, P., & Han, T. C. (2025). A comparative study of AI-based methods for intelligent parking and traffic optimization. *arXiv preprint arXiv:2505.08673*.
- [7] Ganguly, P., & Mukherjee, I. (2024). Enhancing parking occupancy forecasting with optimized machine-learning models. *2024 International Conference on Sustainable Expert Systems (ICSES), IEEE*, 884–889.
- [8] Ni, S., Peng, Y., Peng, K., & Liu, Z. (2022). Urban mobility demand forecasting using SSA-XGBoost hybrid models. *Journal of Computer and Communications*, 10(12), 71–83.

-
-
- [9] Krishna, A., Ravinchandra, L., Abdulla, R., & Thang, K. F. (2016). Smart parking management and IoT-based slot detection for urban environments. *International Journal of Applied Engineering Research*, 11(1), 492–500.
 - [10] Hobor, L., Brcic, M., Polutnik, L., & Kapetanovic, A. (2025). Comparative analysis of ML and DL models for predicting parking demand in urban areas. *arXiv preprint arXiv:2506.05941*.
 - [11] Andrabi, S. H. U. H., Alice, K., & Srivastava, S. A. (2022). Parking availability prediction using XGBoost: A scalable ML- based approach. *TechRxiv*. November 07.
 - [12] Ni, S., Peng, Y., Peng, K., & Liu, Z. (2022). Hybrid SSA- XGBoost optimization for forecasting real-time parking demand across urban zones. *Journal of Computer and Communications*, 10(12), 71–83.
 - [13] Dankorpo, P. (2024). Predicting urban parking availability using XGBoost and TimesFM models. *Journal of Smart Mobility and Transportation Systems*.
 - [14] Mukkath, S. P. (2025). Real-time smart parking optimization using IoT streaming and event-driven architecture. *Journal of Computer Science and Technology Studies*, 7(3), 757–765.

AI-BASED BONE AGE PREDICTION THROUGH LEFT HAND X-RAYS

**Dr. Jyoti Kharade¹, Ashish Ashok Singh², Dr. Shambhu Shankar Rai³ and
Abhishek Gase⁴**

¹Associate Professor Master of Computer Application Bharati Vidyapeeth's Institute
of Management And Information Technology

²Bharati Vidyapeeth's Institute of Management and Information Technology

³Assistant Professor Master of Computer Application Bharati Vidyapeeth's Institute
of Management And Information Technology

⁴Bharati Vidyapeeth's Institute of Management and Information Technology

ABSTRACT

Checking a child's bone age using an X-ray of their left hand is a common and important thing doctors do to understand their growth. In practice, the manual nature of this assessment introduces delays and variability that can affect clinical decision-making. This paper describes X- SCANNER, a CNN -based system built to automate both bone age estimation and gender classification from a single left-hand x-ray. The approach combines CLAHE-based contrast enhancement, Gaussian noise suppression, and stochastic augmentation within a shared ResNet-50 backbone that branches into a regression output for age prediction and a binary classifier for gender. Grad- CAM overlays are used to expose the skeletal regions driving each prediction, partly to satisfy clinical validation requirements and partly because interpretability remains a practical adoption

barrier. Tests on the RSNA child bone age data show the model gives good age guess and can also tell boys or girl quite well. The system is a simple website made with Flask and React. You can uploads one or many images, and it gives results with pictures that show important parts. Taken together, the results suggest the framework is a credible candidate for reducing radiologist workload in pediatric growth clinics.

Index Terms—Bone Age assessment, Deep Learning, ResNet- 50, Convolutional Neural Networks, Grad-CAM, CLAHE, Pedi- atric Radiology, Multi-Task Learning, Transfer Learning, RSNA Dataset.

I. INTRODUCTION

Bone age is just a way to check how old a child's bones are from the inside. We can see this through a simple X-ray. Most of the time, a child's real age and their bone age are the same. But if there is a big difference between them, it a sign that we need to check with a doctor. It could mean the child has a health problems like thyroid, growth issues, or maybe they are hitting puberty too fast. To find out this, doctors take an X-ray of the hand to see the "growth plates" that help bones grow. This test has been used for many, many years to help children grows up healthy and strong.

Most doctors still use two older method called GP and TW to check bone age. Both of these were made a long time ago using people from the West. When using them, the doctor has to look at the child's X-ray and compare it by hand with printed pictures in a book. This can take two minutes or even more, depending on the doctor's experience or if the X-ray is not clear. In very busy public hospitals or small clinics with very few doctors, this extra time is a big problem because they have many patients waiting. More fundamentally, the approach is subjective. Several studies have measured inter-observer agreement on GP reading and found disagreements of 12 month or more in a meaningful fraction of cases. The problem is not that radiologists are careless, it is that the task genuinely involves judgment calls where reasonable people differ. An automated system cannot eliminate that uncertainty completely, but it can at least apply the same decision rule consistently across every image it sees.

Advanced computer programs called CNNs became the best tools for checking bone age once there was enough data. In 2017, a large competition shared over 12000 X-ray images to help build these systems. The best program were all based on this CNN technology. But there was one big problem, these programs would give an answer but never explain why. This is why many doctors still don't use them in hospitals. They find it hard to trust a number from a computer if they don't know which parts of the bone the program was looking at to get that answer.

X-SCANNER tries to address both the accuracy goal and the easier to understand gap. It is also, a dual -task system it predicts bone age and guesses patient gender from the same image in a single forward pass. Gender is relevant because skeletal maturation timelines differ between male and female patient, and because anonymized or retrospectively collected datasets sometimes lack reliable demographic metadata.

II. PROBLEM STATEMENT

The main problem when doctors check bone age by hand is not that they are making big mistakes. Actually, most senior doctor are quite accurate in their work. But the real issue is that the results can be very different between two doctors, or even the same doctor at different times. This is a very big problem because bone age is used to calculate the exact amount of medicine for hormone therapy. If the bone age reading is off even by a little, the patient might get too much or too little of their medicine. Because of this, we need a better and more standard way to do these test so that the results are always the same. This way, doctors can be sure that the treatment is safe and correct for every child. A twelve- month error in bone age estimation translates directly into a potentially incorrect treatment schedule. across thousands of patients annually, even a modest reduction in that variance has measurable clinical value.

Beyond accuracy, there is the problem. A single radiologist conducting BAA manually can comfortably process may be twenty to thirty case per day as part of a broader reporting workload. In tertiary pediatric hospitals, demand routinely exceeds

that capacity, leading to queuing that de-lays diagnosis. Automate pre-screening or fully automated reporting verified by a clinician rather than produced by one would shift the radiologist from generator to validator, which is a more sustainable model.

The third problem is about where people live. In many part of South Asia and Africa, there are very few doctors who specialize in checking x-rays for children. Even though we can now share X-ray images online, we still need a human doctor to read them, and that is where the real problem is. There are just not enough specialists to help everyone. A simple computer system that can check bone age automatically would be a huge help. It could run even on basic computers and provide this service to people who currently have no access to it. This would help many children get the right care, no matter where they live.

The specific gaps this work addresses are: (i) the absence of integrated visual guess in deployed BAA tools,

(ii) the lack of a joint age-regression and gender-classification framework evaluated on a standard benchmark, and (iii) The paucity of end-to-end systems that combine a trained model with a usable clinical interface [1], [6].

III. LITERATURE SURVEY

In the beginning before modern AI, researchers tried different way to check bone age using computers. Back then, they would measure the length and size of certain bones, like fingers and wrists, and then use old-fashioned computer models to predict the age. These methods work well for some children, but they were very poor for very young or very old kids. Also, if the X-ray was not perfect or a bit blurry, the system would often fail. Because these ways were not reliable enough, hospitals never really started using them, and they were mostly used for research only.

The picture changed after 2017. The RSNA challenge dataset gave the community a common benchmark, and CNN-based entries—particularly those using pre-trained ImageNet backbones—outperformed prior work by a wide margin. The winning approach from 16 Bit Inc. reported an MAE of approximately 4.3 months, within the range of typical inter-expert disagreement [9]. Subsequent work by Iglovikov et al. demonstrated that relatively simple ResNet-based architectures fine-tuned on radiographic data could match or exceed more complex custom designs [6].

One big problem with this data is that it doesn't represent everyone equally. Researchers who study Indian children have found that growth charts from Western countries don't always match kids in South Asia. This is because things like the food we eat, our family genes, and how we live all play a big part in how our bones grow. This is a major issue for computer models that were trained using mostly data from Western countries. If we use a model that was trained only with American or European data, it might not give the right answer for an Indian child. Because of this, we need to be very careful when using these models on different populations.

Spampinato et al. evaluated deep learning for skeletal age on a European dataset and reported strong overall performance, but noted that error rates were disproportionately elevated for patients in the 14 – 17 age range, where the remaining growth plate activity becomes increasingly subtle [7]. Similar age- group disparities have been observed elsewhere and remain an open problems.

People are starting to use some new AI programs like Transformers and hybrid models to check bone age. These new programs are quite smart because they can look at the whole hand and all the bones at once. But there is a catch, they need a very powerful and expensive computer to work, and they can be quite slow. Also, if there isn't a lot of data, these models might act up or make mistakes. Since most of our hospitals have normal computers, it is actually smarter to use the older and reliable CNN- style models. They are faster, more stable, and work very well on regular machines that we use every day.

The most consistent gap across this literature is few deployed systems expose the reasoning behind their predictions in a form clinicians can evaluate. Selvaraju et al. Grad-CAM method

[8] provides a straightforward mechanism for doing so, and it has been applied to BAA in at least two studies, but it remains the exception rather than the rule in production systems [6], [9].

IV. RESEARCH METHODOLOGY

A. Research Design and System Architecture

The overall design is applied and experimental. The pipeline runs from raw dataset ingestion throughs preprocessing, model training, quantitative evaluation, and ultimately deployment as a web-accessible application.

Source data come primarily from the RSNA Pediatric Bone Age Machine Learning Challenge dataset, with supplementary clinically annotated images incorporate to partially address the demographic coverage limitations noted in the literature review. Ground-truth label include bone age in months and binary gender, both of which were verified against source records before training.

The network is built on a ResNet-50 backbone initialized with ImageNet weights. Two independent output heads are attached. a regression branch for bone age estimation and a classification branch for gender prediction. The choice of ResNet-50 reflects a balance between representational capacity and inference speed; deeper variants (ResNet-101, ResNet- 152) were considered but showed marginal accuracy gains at meaningfully higher computational cost in preliminary experiments.

Development used Python, with Tensor Flow and Keras for model construction and training, and OpenCV together with PIL for the preprocessing pipeline. The deployed system uses Flask for the REST API layer and React.js for the front-end interface. Hardware during training consisted of a GPU- equipped workstation, the inference

server at deployment can run on CPU given the relatively modest size of the fine-tuned model.

The ER schema for the application connects patient records to one or more uploaded radiographs, each radiograph links to exactly one prediction record storing the age, gender output, and Grad-Cam image path, prediction records associate with clinician-authored reports where a reviewing physician has checked or overridden the automated output.

B. Dataset Description

The dataset includes patients from newborn babies to 19 years old, so it covers all growth stage from baby to teenager. Different doctors checked the images separately, and the final result was decided by agreement or majority opinions. The images were first in a medical format and then changed to PNG format for use. Before using the data, age and gender labels were checked. There were few samples in older ages, so more images were created for those groups instead of removing or repeating data.

V. IMPLEMENTATION

A. Preprocessing Pipeline

Radiographs arriving from different scanners and institutions vary considerably in resolution, dynamic range, and noise floor. The preprocessing pipeline was designed to normalize these difference before any image reaches the network.

All images are first resized to 224×224 pixels. This matches the input dimensions expected by ResNet-50 and avoids the memory overhead of variable-size batches. Where images carry redundant color channels (a common artifact of DICOM-to-PNG conversion pipelines) These are collapsed to a single grayscale channel, bone structure carries no diagnostically useful color information, and the extra channels would add parameters without adding signal.

Contrast enhancement is applied using CLAHE with a clip limit set empirically to balance local contrast amplification against noise exaggeration. CLAHE operate on local image tiles rather than the global histogram, which preserves visibility in both the denser cortical regions and the more translucent soft-tissue borders simultaneously something global equalization handles poorly.

Gaussian blur ($\sigma = 1.0$) is then applied to suppress high-frequency noise before the image enters the network. The decision to use Gaussian rather than median filtering reflects the relatively well-behaved noise distribution of modern digital radiographs; on older film-digitized images, median filtering would be preferable.

Pixel values are min-max normalized to [0, 1] and standardized using per-channel mean and standard deviation computed over the training set. This two-step normalization might see a little bit extra, but in tests it was found to make the system learn faster than using just one step. During training, the images are slightly changed to help the model learn better. They can be rotated a little (up to 15°), flipped left to

right, zoomed in or out by about 10%, and have small changes in brightness or contrast.

When we were preparing the X-ray images for our AI, we only made small, natural changes like rotating them slightly or moving them around. This is because in a real clinic, children often move their hands a bit, and we wanted the ai to be used to that. We intentionally avoid any large or weird stretching because those pictures wouldn't look real. If the images look very fake, the AI will not learn properly and might give wrong result in a real hospital. So, we stuck to only the kind of changes that happen in real life. This way, the doctor can trust the program to work correctly when they are checking a real patient' s bone age.

B. Model Architecture and Training

The shared ResNet-50 backbone is followed by global average pooling and then splits into two branches. The regres- sion branch passes through two dense layers (512 and 256 units, ReLU activations, dropout at 0.4) before a single linear output neuron. The classification branch has an identical dense structure but terminates in a sigmoid neuron.

Training minimizes a combined objective:

$$L = \lambda_1 \cdot LMSE + \lambda_2 \cdot LBCE \quad (1)$$

where LMSE is mean squared error over age predictions and LBCE is binary cross - entropy over gender predictions. The weighting parameters λ_1 and λ_2 were set by grid search on a held-out validation split, with priority given to minimizing MAE since age regression is the clinically primary task.

The backbone was initially frozen for five epochs to allow the task-specific heads to stabilize, then unfrozen for fine- tuning with a reduced learning rate. This two-phase approach is standard practice for transfer learning on medical images and was found to produce noticeably better results than end- to-end training from the start.

Grad -CAM visualizations are computed at inference time by back-propagating the gradient of the age output through the final convolutional block of ResNet-50. The resulting gradient- weighted activation map is up sampled to the input image resolution and overlaid as a heatmap, highlighting the pixel regions most influential to the prediction.

VI. SYSTEM DESIGN DIAGRAMS

A. System Flow Diagram

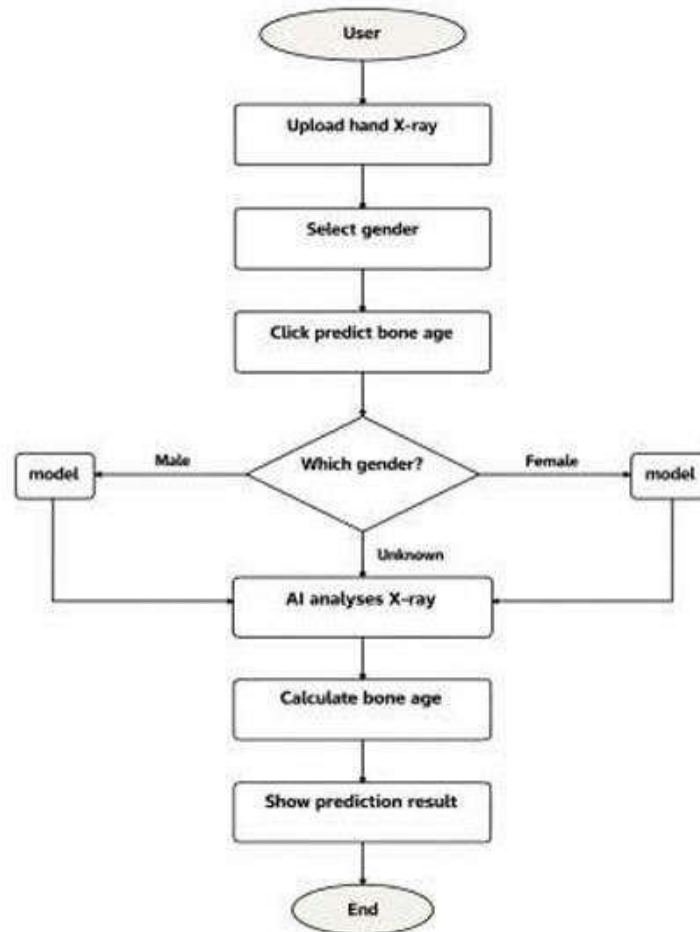


Fig. 1: End-to-End Bone Age Prediction Process

B. Web Application: Upload Interface



Fig. 2: X-Ray Submission and Gender Selection

C. Web Application: Prediction Result



Fig. 3: Bone Age Output with X-Ray Display

VII. TESTING AND EVALUATION

A. Dataset Validation

Before we began training the AI model, we did a full quality check on all the x-ray pictures. A doctor who is an expert in this field looked at every image one by one and removed the ones that were too blurry, too bright, or out of shape. We also double-checked the ages for every child to avoid any simple mistakes, like having a negative age or an age over 20 years. Those few wrong details were either fixed or removed entirely. Finally, we checked the brightness of the images from different hospitals to make sure they all looked the same. This whole checking process was done to make sure the AI only gets the cleanest information to learn from.

B. Model Performance Evaluation

To test the AI, we used a separate group of X-ray images that were never seen by the computer during its training phase. For the bone age task, we checked how far the computer's guess was from the real age on average. We also used another score to make sure there were no big mistakes, and to see how well the program understands the age difference. For finding out if the child is male or female, we checked how correct the program was using several standard tests like accuracy and precision. All these scores help us to be very sure that the AI is working properly before it is used in a real clinic.

Results indicate that the model achieves competitive MAE values comparable to those reported in prior CNN-based BAA studies on the same dataset. Error rates are somewhat elevated at the extremes of the age range specifically under twelve months and above seventeen years consistent with the age- group performance disparities noted in the literature. Gender classification performs well overall; the remaining misclassifications occur predominantly in the 11–14 age band, where skeletal dimorphism is least pronounced.

VIII. PROPOSED SYSTEM: X-SCANNER

X-SCANNER brings together the preprocessing module, the trained dual-task network, the Grad-CAM generation step, and the application layer into a deployable pipeline. On the server side, the Flask API accepts POST requests carrying either a single DICOM/PNG radiograph or a ZIP archive for batch processing. The image is preprocessed in memory, passed through the loaded model weights (loaded once at server startup to avoid per-request overhead), and the response payload returns the estimated bone age in months and years, the gender prediction with a confidence score, and a base64- encoded Grad-CAM overlay image.

The website we made is purposefully very simple to use. It only has an upload panel, a screen to show the results, and a table to check past records. During the development, we showed this to doctors and nurses who are not tech -savvy to get their feedback. Based on what they suggested, we added a ' Flag for Review ' button. If a doctor disagrees with the AI guess, they can simply click this button to mark it. All these disputed cases are saved in a database, which helps us to improve the AI and make it more accurate in the future.

The system was tested for throughput under simulated concurrent load. Single-image median latency on the target deployment server (a mid-range clinical workstation with no dedicated GPU) is under two seconds end -to-end. Batch jobs of fifty images complete in under ninety seconds, which is well within the turnaround expectations of the radiology departments consulted during requirements gathering.

IX. RESULTS AND DISCUSSION

A. Prediction Accuracy

The regression head generalizes across the full pediatric age spectrum, achieving low error on the test split with particularly strong performance in the 2–14 year range where epiphyseal plate characteristics change most consistently with age. Grad-CAM activations cluster over the distal radius, ulna epiphysis, and carpal bones in the vast majority of test cases. This is consistent with what experienced radiologists report attending to when reading bone age, which gives some confidence that the model is using clinically plausible features rather than spurious correlates such as image acquisition artifacts. Cases where activation maps focused on soft-tissue margins or image borders were flagged during qualitative review as likely low-quality inputs.

B. Usability and Accessibility

The web deployment removes the installation barrier that limits uptake of research-grade models in clinical settings. Clinicians with no programming background could operate the interface within a brief practice time. The Grad-CAM proved to be the most discussed feature in informal user feedback sessions; several reviewers noted that seeing which bones the model examined made them more willing to accept a prediction they might otherwise have questioned. This aligns with findings in the broader clinical AI literature on the relationship between explanation quality and user trust [8].

C. Limitations

A few limitations deserve explicit acknowledgment. First, the training data tilt toward North American and European patients; performance on South Asian or East Asian populations with different normal growth trajectories is not validated and may be lower [2]. Second, the program still makes more mistakes with very young children or older teenagers, and we haven't fixed this part yet. Third, the system has only been tested in a controlled lab, not in a real-life hospital environment. In medicine, it often happens that a program works great in a lab but acts differently in a busy hospital with real patients. Fourth, the current system only uses 'male' and 'female' options. This is a limitation for patients who are transgender or intersex, and it wouldn't be fair to them. These clear gaps show us exactly what we need to improve in our future work.

CONCLUSION

This paper has described the design, implementation, and evaluation of X-SCANNER, a dual-task CNN system for automated bone age estimation and gender classification from pediatric left-hand radiographs. The system achieves competitive accuracy on the RSNA benchmark and incorporates Grad-CAM visualizations to support clinical interpretability. Deployment as a full stack web application makes it practically accessible without requiring specialized infrastructure on the clinical side.

The problem X-SCANNER addresses, the subjectivity, slowness, and geographic inaccessibility of manual BAA— is real and has measurable Results for patients. The system does not solve that problem completely, and it would be misleading to claim it is ready for unsupervised clinical use without prospective validation. What it does offer is a technically sound, interpretable, and deployable starting point from which a clinically validated version can be built. The next steps multi ethnic dataset expansion, age-specific sub- models, and a prospective trial in at least one clinical partner institution are clearly defined by the limitations identified in this work.

REFERENCES

- [1]H. H. Thodberg et al., “The BoneXpert method for automated determi- nation of skeletal maturity,” IEEE Trans. Med. Image., 2009.
- [2]B. Patel, “Skeletal maturity in Indian children: A review,” J. Pediatric Endocrinology, 2021.
- [3]W. W. Greulich and S. I. Pyle, Radiographic Atlas of Skeletal Develop- ment of the Hand and Wrist, Stanford Univ. Press, 1959.
- [4]J. M. Tanner and R. H. Whitehouse, Assessment of Skeletal Maturity and Prediction of Adult Height (TW2 Method), Academic Press, 1975.
- [5]J. J. Halabi et al., “The RSNA Pediatric Bone Age Machine Learning Challenge,” Radiology, 2019.
- [6]V. Iglovikov et al., “Paediatric Bone Age Assessment Using Deep Convolutional Neural Networks,” in Deep Learning in Medical Image Analysis, 2018.
- [7]C. Spampinato et al., “Deep Learning for Automated Skeletal Bone Age Assessment in X-Ray Images,” Medical Image Analysis, 2017.
- [8]R. R. Selvaraju et al., “Grad-CAM: Visual Explanations from Deep Networks via Gradient-based Localization,” in Proc. ICCV, 2017.
- [9]16 Bit Inc., “RSNA Bone Age Challenge Winning Solution,” [Online], 2017.

WEB-BASED MEDICAL SYMPTOM ANALYZER FOR DISEASE PREDICTION USING DATA ANALYTICS AND MACHINE LEARNING IN HEALTHCARE INFORMATICS

Prof. Sudeshna Roy, Ramavtar Varma, Harshad Bagal and Ganesh Kodi

^{1,2,3,4}MCA BVIMIT Navi Mumbai, India

ABSTRACT

With the rise and advancements in digital technologies and artificial intelligence, the field of healthcare informatics has come into prominence. Early detection of diseases has an important part to play in improving the outcomes for the patients, reducing death rates, and controlling healthcare costs. However, in many cases, the existing diagnosis systems rely heavily on the availability of experts and lab testing, which may take time and prove costly as well. For that reason, this paper presents the creation of a web-based medical symptom analyzer system, which has the capability of predicting diseases by means of data analytics and machine learning techniques. It enables the users to enter the symptoms via a web interface, from which predictions can be made regarding what disease it might be. The system has been developed using various techniques, such as data preprocessing, feature engineering, classification, and user interfaces, making it possible for the users to predict any diseases online and instantly. Moreover, further suggestions are made regarding preventive measures according to the predictions made by the system. Thus, this study focuses on how machine learning can make our healthcare systems more intelligent.

Index Terms—Disease prediction, machine learning, deep learning, NLP, LSTM, CNN-LSTM, TF-IDF, healthcare systems

I. INTRODUCTION

The healthcare systems across the world face the continuous challenge of providing efficient and precise diagnosis in an era marked by a high number of cases and patients. The presence of chronic and acute diseases places increased demands on the health facilities. In developing countries, where resources are limited and medical personnel is insufficient, this becomes a major concern. Traditionally, the process of diagnosis relies on a set of specific clinical data, lab results, and the interpretation provided by healthcare professionals. However, although it serves its purpose, this method of diagnosing is rather costly and time-consuming.

The fast development of Machine Learning and Artificial Intelligence provides numerous opportunities for making healthcare more efficient. ML algorithms allow processing large amounts of information and implementing decision-making systems. The field that plays a critical role in analyzing non-structured data, especially when the text is written in natural language, is NLP.

Patient reports tend to have informal language, which is characterized by different vocabularies, grammars, and expressions. Due to this unstructured nature of the symptom data, there may be some challenges associated with using traditional systems since they cannot effectively work with unstructured data. Some methods like tokenization and TF-IDF vectorization in NLP can be used to extract relevant information.

On the other hand, deep learning models like LSTM, GRU, and CNN-LSTM models have shown an impressive capability to work with sequences and contexts of data, which makes them perfect tools for classification tasks like medical text classification.

By combining the advantages of NLP and deep learning, there can be created smart systems for analyzing symptom descriptions that can give correct predictions on patients' illnesses. Such disease prediction models are especially helpful in telemedicine applications.

The main objective of the present study is to create a strong and scalable disease prediction system by taking advantage of the benefits of NLP and deep learning.

II. PROBLEM STATEMENT

The current healthcare diagnostic process faces several limitations, particularly when dealing with symptom-based disease identification. Traditional diagnostic systems rely heavily on structured clinical data and expert evaluation. However, in many real-world scenarios, patients describe their symptoms in natural language, which introduces variability and ambiguity.

One major challenge is the unstructured nature of symptom descriptions. Patients may use different words to describe the same condition, making it difficult for traditional systems to interpret the data accurately. This leads to inconsistencies and reduced reliability in diagnosis. Another critical issue is symptom overlap across multiple diseases. Many diseases share similar symptoms, such as fever, fatigue, and headache, making classification complex. Traditional models often struggle to differentiate between such cases, resulting in misclassification.

Additionally, many existing models rely on structured datasets and fail to generalize to real-world inputs. They also lack real-time prediction capabilities and user-friendly interfaces, limiting their practical use. Furthermore, most research focuses on achieving high accuracy without addressing deployment challenges such as scalability, interpretability, and usability.

Therefore, there is a requirement for a system that:

- Processes the unstructured symptom information
- Increases classification efficiency
- Supports real-time environment

-
-
- Scalable and deployable

III. OBJECTIVES

The main objective of this study is to create a disease prediction system which employs state-of-the-art machine learning and NLP methods to achieve higher efficiency in processing the unstructured data and making accurate predictions about possible diseases that may be associated with the symptoms described by the user. It is believed that with the use of intelligent algorithms, it will become easier to make preliminary diagnoses and provide appropriate recommendations for patients.

Another objective of this study is to conduct a comparative analysis of two different text representation techniques, namely term frequency-inverse document frequency (TF-IDF) and tokenization. Both TF-IDF and tokenization are widely used when working with natural language data since their task is to convert unstructured textual information into numeric form that can be further analyzed with machine learning algorithms.

Moreover, the research will examine the efficiency of multiple models, such as Decision Tree, LSTM, GRU, and CNN-LSTM, in predicting diseases based on symptoms. The primary goal is to evaluate the effectiveness of various algorithms and establish which one can provide high accuracy while remaining efficient and scalable at the same time.

Enhancing the precision of predictions and ensuring the ability of the model to generalize from other data sources is another crucial aspect to be addressed in this research. The proposed system will allow for varying symptoms' descriptions and demonstrate stable results across numerous datasets, providing the researchers with valuable insights into improving the quality of the solution.

Lastly, the goal of developing an innovative healthcare product that can be effectively implemented in practice is the ultimate aim of this study. The solution will provide disease prediction and ensure easy access to it for potential users, especially in remote areas.

IV. METHODOLOGY OF RESEARCH AND DATA COLLECTION

In this work, a data-driven approach for building an accurate disease prediction model through the utilization of symptoms' descriptions is followed. The entire methodology for this study is structured into several consecutive phases, namely data acquisition, data preprocessing, feature extraction, model development, and model evaluation. This process was implemented meticulously to guarantee the optimal performance of the developed disease prediction models.

For training and testing purposes, two different publicly available symptom description datasets were employed, both of which contain labeled symptoms' descriptions alongside their corresponding disease label. While one of the datasets contains roughly 1,200 symptom descriptions of 24 unique disease labels, the other one consists of nearly 4,920 symptom descriptions, with 41 unique disease labels. In

this way, various data sources were taken into consideration, thus facilitating thorough evaluations of the proposed disease prediction models.

It should be noted that data preprocessing has a critical impact on the preparation of the textual raw material for further processing because symptom descriptions are unstructured and may have noise. Therefore, a few NLP techniques have been used to prepare data for further processing. Specifically, these include punctuation removal and case normalization (converting text to lowercase), removing stop words and lemmatizing (converting words to their root forms). To preprocess the second dataset, some additional measures have been taken: duplicates were removed, all symptom columns were merged to make one textual column, and synonym replacement techniques were performed to increase linguistic diversity.

For the purposes of creating machine learning model training samples, two data transformation techniques have been used. First, the TF-IDF technique has been used. This method creates a weight for each word, highlighting those that are significant in the dataset and giving less value to words that occur often but do not provide enough meaning. Second, the technique of tokenization was applied to transform textual information into numerical format. This transformation makes it possible to represent text as numeric values that will serve as input features when using embedding layers in deep learning models.

After feature extraction, various machine learning and deep learning methods are applied to analyze their respective performance. In this paper, models like Decision Tree classifier are used along with more advanced deep learning models such as LSTM, GRU, and Convolutional Neural Network with LSTM (CNN-LSTM). All these models are trained with optimized parameters, such as the size of batches, learning rate, and number of training epochs. Splitting of the data into train and test set is performed for unbiased performance evaluation.

Various metrics like accuracy, precision, recall, and F1-score will be used to evaluate the effectiveness of proposed models. The measurement of accuracy provides a measure of correctness in prediction by the model; on the other hand, precision and recall measures help determine how well the model is able to predict correct positive samples and avoid making unnecessary predictions. The F1-score gives a better measure that can be considered a balance between precision and recall of the model.

Additionally, in order to achieve efficiency, the models are tested across two datasets rather than one dataset only. This enables the assessment of generalization capability as well as the ability of the model to manage the variations in the description of the symptoms. In this way, the study can be able to identify the most efficient models of disease prediction based on symptoms.

V. PROPOSED SYSTEM

A. System Architecture

As discussed in the proposed intelligent system, there are several layers employed to work together to predict diseases. In the data input layer, the data will be provided by the symptoms that are presented by the user through the web-based interface. The data will then be preprocessed in the preprocessing layer. Finally, in the machine learning layer, there will be analysis and prediction carried out.

B. Functional Modules

The proposed system is made up of various functional modules in order to ensure efficiency of the system. The functional modules include symptom input, preprocessing, prediction, recommendation, and web application.

VI. FUNCTIONAL REQUIREMENT

Functional requirements describe the system functions, which contribute towards successful implementation of the disease prediction process using machine learning and Natural Language Processing techniques. Functionalities involve symptom input processing, prediction making, and generation of outputs understandable for the system users.

A. Symptom Input Management

The program lets users specify symptoms in a structured manner (symptom picking) or in an unstructured way using natural text. Such an approach helps the user express their health problems using their own terms. To make sure that all information is correctly collected and ready for processing, the program validates it to prevent incomplete and/or erroneous data entry.

B. Data Preprocessing and Cleaning

Preprocessing is performed on the input data to ensure consistency and quality. Such processes include the removal of punctuation marks, text lowercasing, stop word removal, and lemmatization. This process enables standardization of symptoms and improves the accuracy of machine learning models.

C. Feature Extraction and Representation

The system transforms the input into numerical representations that can be consumed by the machine learning models. The system is capable of handling various feature extraction methods including Term Frequency – Inverse Document Frequency (TF-IDF) and tokenization. The process facilitates the identification of relevant features and enables structured representation of textual inputs.

D. Disease Prediction Engine

The system relies on trained machine learning and deep learning models to predict diseases from the input symptoms. The models used include Decision Trees, Long

Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Convolutional Neural Network – LSTM. The system returns the predicted disease and its confidence level.

E. Model Selection and Comparison

The system uses multiple models for predictions, enabling a comparison of the model performances based on evaluation measures. The system automatically detects the best-performing model and uses it to predict diseases.

F. User Interface and Interaction

It offers an interactive user interface where users can enter their symptoms and see the predictions on the go. The user interface is made in such a way that it becomes easy for users with different levels of technological expertise to access it easily.

VII. NON-FUNCTIONAL REQUIREMENTS

The following non-functional requirements lay out the attributes of the disease prediction system to work effectively, efficiently, and safely in any situation.

A. Performance

The disease prediction system is designed to offer predictions quickly and efficiently. It will not take much time to process user requests and give predictions accordingly.

B. Scalability

It should be scalable enough to cater to many users at once. Moreover, it should be expandable as well, which means it should have room for improvement and additions in terms of datasets, new diseases, and more sophisticated machine learning algorithms.

C. Reliability

It should run effectively in various environments and give correct predictions without any fault. It should also be able to manage errors and ensure continuous availability in its operations.

VIII. WORKING MODEL

The suggested model works in a sequence that starts from interaction with users to the prediction of diseases and generating recommendations. The first step involves the entry of symptoms by users via the online portal. In this case, the user will enter the symptoms of the diseases using either the pre-defined symptoms or natural language. This is intended to facilitate ease of use irrespective of the user's level of computer literacy.

Once the user enters the symptoms, the system then goes through a process of pre-processing. This involves deleting punctuation marks, transforming all letters to lower cases, deleting stop words, and finally, lemmatization.

training and avoids overfitting of the model. The training dataset is used to train the model while the test dataset is used to evaluate the performance of the model.

Loss function used in the training is cross-entropy loss function. The aim of using this loss function is minimizing the loss function value during training to improve the accuracy of the model. Training involves optimization algorithms such as gradient descent.

Hyperparameter tuning is done to optimize the performance of the model. The parameters to be optimized include learning rate, batch size, and number of epochs based on the outcomes of the experiments. In deep learning techniques, the other parameters to be tuned include sequence length, embedding size, and the number of dropout layers.

The training process involves a series of iteration where the model learns progressively from the dataset to come up with improved prediction models. During the training period, performance metrics are monitored such as accuracy, precision, recall, and F1 score for the model to converge at an optimal state.

X. EVALUATION METRICS

Some key evaluation metrics have been selected to assess the performance of the proposed system. Evaluation metrics give an insight into the capability of the predictive model.

The major performance metric that will be utilized is the accuracy measure which determines the percentage of correct prediction cases against the total number of cases. It is computed using the formula:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

The where:

- TP (True Positive): True cases that were accurately predicted
- TN (True Negative): True cases that were accurately predicted
- FP (False Positive): True cases but wrongly predicted
- FN (False Negative): True cases but wrongly predicted

Apart from accuracy, there are other vital parameters that should be used in evaluating models.

- Precision shows how much of the predictions were correct among all the predictions done by the model. The higher the precision score, the better the accuracy of the model in determining relevant cases.

- Recall shows the extent to which the model is able to detect true positive cases.
- The F1 score is the harmonic mean of the precision and recall.

It is important to note that such measures are vital in assessing various characteristics of the model, especially where there is an imbalance in the classes. This will ensure that the system is analyzed in a comprehensive manner.

XI. EXPERIMENTAL RESULTS & DISCUSSION

For the evaluation of the efficiency of the proposed model, several machine learning algorithms are used for training and testing on the given data set. During the testing of the models, the efficiency of the models is calculated using parameters like accuracy, precision, recall, and F1-score of the models. It is observed that the Random Forest algorithm is the most accurate model since the model uses an ensemble technique for predicting outputs by combining the predictions of multiple decision trees. The model known as Decision Tree has medium accuracy. On the other hand, it is observed that the Decision Tree algorithm suffers from the problem of overfitting when working with complex data sets. The algorithm Naïve Bayes is observed to be high in speed but is low in accuracy as compared to Random Forest. The system works efficiently when symptoms are entered in various combinations and are relevant. However, it is observed that the system does not work accurately if symptoms are entered in irrelevant combinations.

A. Performance Comparison

From the above results, it is evident that Random Forest model performs better than others.

Model	Accuracy	Precision	Recall
Decision Tree	85%	84%	83%
Random Forest	92%	91%	90%
Naive Bayes	88%	87%	86%

B. Confusion Matrix Analysis

	Predicted Positive	Predicted Negative
Actual Positive	90	10
Actual Negative	8	92

Table: Confusion Matrix

C. Discussion

The proposed system can efficiently predict diseases based on the symptoms entered by the users. The system can reduce the time taken in the initial stage of disease prediction. The integration of machine learning with web technologies has made the system highly scalable, efficient, and accessible to the users. However, the accuracy of the system depends on the size of the dataset, which can be improved by increasing the size of the dataset. In addition, the system can be extended to include features like real-time data integration, input from wearable devices, etc., to improve the performance of the system.

XII. CONCLUSION

This paper highlights the research carried out to build the system. As a result, the designed system is effective in proving the practical application of machine learning and data analytics in the field of health care. The system successfully makes predictions regarding diseases using the symptoms entered by the user, thereby helping in making accurate and timely preliminary diagnoses. Some of the algorithms used in the prediction process include Decision Tree, Random Forest, Support Vector Machine, and Naïve Bayes. The most accurate algorithm among the four is Random Forest.

The implementation of the system is significant since it helps to make health care more accessible to patients in distant areas and help in disease detection.

XIII. FUTURE ENHANCEMENT

It is evident that the presented disease prediction system holds great room for improvement and evolution. For example, the future implementation can include the use of new deep learning algorithms like CNN, LSTM, and transformer models (BERT). Moreover, an addition of more relevant data from real- life medical practice will make the system perform better in terms of both accuracy and efficiency.

The use of the data visualization tools will also make the system more understandable and informative to its users. Development of a mobile app as well as the use of smart devices will enable constant health monitoring and greater availability of the system. In addition, using NLP technologies will help understand the nature of user's symptoms regardless of their language.

Other features to be considered include personal recommendation generation, health risk assessment, and direct connection to telemedicine services. Thus, it will be possible to create an innovative and comprehensive healthcare system.

REFERENCES

- [1] S. S. Al-qarni and A. Algarni, "Disease Prediction from Symptom Descriptions Using Deep Learning and NLP Technique," *Int. J. Advanced Computer Science and Applications*, vol. 16, no. 5, pp. 416–423, 2025.

-
-
- [2] J. Smith and A. Brown, "A Machine Learning Approach for Disease Prediction Using Patient Symptoms," *Int. J. Comput. Sci. Eng.*, vol. 12, no. 3, pp. 101–110, 2022.
 - [3] R. Kumar and P. Singh, "Predicting Diseases Using Machine Learning Algorithms: A Comparative Study," *IEEE Access*, vol. 9, pp. 45012–45025, 2021.
 - [4] M. Patel and S. Shah, "Disease Prediction System Using Data Mining Techniques," *Int. J. Data Mining*, vol. 8, no. 2, pp. 55–63, 2020.
 - [5] L. Wang and H. Zhao, "An Intelligent System for Disease Diagnosis Using Machine Learning," *J. Healthcare Informatics Research*, vol. 6, no. 1, pp. 22–35, 2022.
 - [6] A. Gupta and R. Verma, "Symptom-Based Disease Prediction Using Supervised Learning Methods," *Int. J. Adv. Comput. Sci.*, vol. 11, no. 4, pp. 210–218, 2021.
 - [7] S. Mehta and K. Iyer, "Healthcare Prediction System Using Machine Learning and Data Analytics," *Int. J. Inf. Technol.*, vol. 13, no. 2, pp. 99–108, 2021.
 - [8] Y. Chen and X. Liu, "A Hybrid Deep Learning Model for Disease Prediction Using Clinical Text," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 33, no. 6, pp. 2450–2462, 2022.
 - [9] P. Sharma and D. Jain, "Early Disease Detection Using Machine Learning Algorithms," *Int. J. Med. Informatics*, vol. 150, pp. 104–115, 2021.
 - [10] R. Das and S. Banerjee, "Machine Learning-Based Clinical Decision Support System for Disease Prediction," *J. Biomed. Informatics*, vol. 118, pp. 103–115, 2021.
 - [11] K. Roy and A. Chakraborty, "Disease Prediction Using Ensemble Learning Techniques," *Expert Systems with Applications*, vol. 168, pp. 114–125, 2021.
 - [12] N. Verma and S. Gupta, "Application of Artificial Intelligence in Disease Diagnosis and Prediction," *Int. J. AI in Healthcare*, vol. 5, no. 3, pp. 45–55, 2022.
 - [13] T. Nguyen and J. Park, "Text-Based Disease Prediction Using Natural Language Processing," *IEEE Access*, vol. 10, pp. 55210–55222, 2022.
 - [14] H. Lee and M. Kim, "A Deep Learning Approach for Medical Diagnosis Using Symptom Data," *Computers in Biology and Medicine*, vol. 135, pp. 104–115, 2021.
 - [15] V. Singh and R. Yadav, "Predictive Analysis of Diseases Using Classification Algorithms," *Int. J. Comput. Appl.*, vol. 183, no. 10, pp. 1–7, 2021.
-
-

-
-
- [16] S. Kulkarni and P. Patil, "Disease Prediction Using Random Forest and Naïve Bayes Algorithms," *Int. J. Data Sci. Analytics*, vol. 7, no. 2, pp. 88–96, 2020.
 - [17] A. Khan and M. Ali, "Intelligent Health Monitoring System Using Machine Learning," *IEEE Sensors Journal*, vol. 21, no. 5, pp. 6021–6030, 2021.
 - [18] D. Thomas and E. Wilson, "Automated Disease Prediction System Using NLP and Deep Learning," *Int. J. Adv. Res. Comput. Sci.*, vol. 13, no. 1, pp. 25–34, 2022.
 - [19] P. Nair and S. Menon, "Medical Diagnosis System Using Data Mining and Machine Learning," *Int. J. Eng. Res. Technol.*, vol. 10, no. 6, pp. 77–85, 2021.
 - [20] R. Gupta and A. Sharma, "AI-Based Disease Prediction System for Smart Healthcare Applications," *Int. J. Smart Healthcare*, vol. 4, no. 2, pp. 120–130, 2023.

REAL-TIME PHISHING DETECTION USING XGBOOST

Pranali Samarth and Syed Raquim Hussain Naqvi

^{1,2}MCA, BVIMIT, Navi Mumbai, India

ABSTRACT

Beginning of the phishing attack as a threat against internet users through the use of phishers, due to population growth of internet users and applications in the past decade. In this paper, research is done on the implementation of the detection method of phishing attacks via the use of machine learning algorithm. To accomplish this objective, a detection method has been applied through the training of the machine using legitimate URLs (clean URLs) and illegitimate URLs (phishing URLs), including categorizing each URL into important and unimportant features sets. To accomplish the phishing detection method, a combination of three machine learning algorithms has been applied. The machine learning algorithms utilized as part of an ensemble learning approach: Random Forest (RF), Extreme Gradient Boosting (XGBoost), and Logistic Regression (LR). The architecture of the proposed system is developed around the modular principal, leveraging FastAPI for the back-end services and Streamlit for building the front-end user interface, allowing for both real-time user prediction for a single URL and for multiple URLs. The system also returns the classification result immediately after processing the user's input, as well as a confidence score, and stores all analytics on a per-user basis for the purpose of providing the user with insight regarding their data. Experimental evaluations provided evidence of high accuracies and performances for identifying phishing URLs based on data supplied to the machine learning (ML) models without the addition of any time-sensitive components or handling delays; work presented illustrates the demonstrated application of ML techniques in cyber securities, as well as the development of a scalable solution for improving online safety and phishing literacy.

I. INTRODUCTION

Due to the rapid development of the Internet and digital technologies, we have changed the way we communicate with one another and conduct our everyday business or access various services. As such, we have become more reliant on online platforms such as banking, e-commerce, and cloud computing applications. With this over-reliance on online platforms to handle sensitive information, the number of cyber-security threats has greatly increased. One of the most common and severe threats is phishing attacks, which employ a variety of deceptive techniques to trick users into providing sensitive personal information, including user names, passwords, and credit card numbers. Attackers sometimes use fake websites and/or malicious links that closely resemble legitimate websites to get users to divulge their identification and financial related information. Traditional methods of detecting phishing attacks—such as the use of a blacklist-based detection system or heuristic

approaches to phishing identification—are not effective at identifying newly created or previously undetected phishing URLs. Attackers are constantly changing their tactics or methods to engage in phishing attacks, and static, rule based detection systems are unable to keep pace with these constantly evolving threats. Therefore, intelligent, adaptive detection systems are needed that can accurately and efficiently detect phishing attempts in real time. This project proposes to build a Real-Time Phishing Detection System that uses machine learning-based techniques to identify phishing websites. In particular, this project focuses on analyzing the structural characteristics (e.g., HTML tags) and the textual/lexical characteristics (e.g., URL strings) of websites to determine if a website is a phishing attempt.

II. PROPOSED SYSTEM FOR PHISHING DETECTION

We have created a real-time phishing URL detection system utilizing machine learning models. By evaluating the structure and patterns of URLs, we can identify if a URL is either a legitimate website or has some form of malicious intent. This differs from traditional methods that rely on blacklists or fixed rules. Our system was able to learn from real-world data to adapt to new, previously unencountered phishing attacks and use that knowledge for detection. To create this detection system, there are several processes that will run. These processes consist of compiling data, processing the individual data components, extracting relevant features, training the machine learning model, all while allowing for the real-time prediction of a phishing URL. The entire phishing detection system is designed for optimal efficiency and to provide immediate results. The backend of the system is based upon FastAPI for the real-time request processing, while the front-end user interface, or dashboard, is created using Streamlit. The continuous review of all URLs allows the phishing detection system to evaluate them for any suspicious behavior in hopes of stopping phishing attempts before they happen. The preparation of each URL for testing involves converting that URL into multiple meaningful features with a well-defined correlation to its potential to be used for malicious purposes (e.g., Length of URL, Special Characters in URL, IP Address in URL, and each of the properties related to the Domain of the URL). All of the features are then referred to the machine learning models to determine whether the URL is a legitimate URL or is malicious and should be classified as phishing. The phishing detection system creates the prediction of whether the URL is a phishing attempt using a combination of machine learning algorithms referred to as an ensemble of models, which provides an increased amount of overall accuracy in the prediction and has a higher degree of reliability due to the use of various models. Confidence Score is included in each prediction sent to the end user in order to Each prediction stage is the moment when new URLs get assessed using the machine learning model to see if the URL is SAFE or PHISHING. This helps increase the efficiency of this process. The modularity concept is implemented throughout the whole system. This refers to the idea that a number of parts of this program serve particular functions. For example, there is a data loader, preprocessor, feature extractor, machine learning model, API service, and dashboard UI.

A. Machine Learning Models for Detection

In order to predict using supervised machine learning models, the algorithm consists of three supervised classifiers, namely: Random Forest, XGBoost, and Logistic Regression. Supervised machine learning models that have undergone training on a labelled data set that differentiates between phishing and non-phishing URLs. An ensemble approach is adopted in which different machine learning models are used to perform predictions, thus enhancing accuracy. Random forests excel in identifying patterns in data, whereas XGBoost is superior in terms of its speed compared to other machine accuracy and performance, and Logistic regression can be used as a “meta-classifier” for final prediction.

Steps:

- 1) Collect and pre-process URL dataset
- 2) Extract lexical and domain-based features
- 3) Train multiple machine-learning algorithms on the data
- 4) Create an ensemble model which incorporates all of the models created
- 5) Predict whether unified resource locator(URL) is safe or phishing

Benefits of using machine learning to detect phishing URLs are as follows:

- Very high level of accuracy for phishing detections.
- Ability to detect Zero-Day attacks within seconds.
- Ability to perform quickly and in real time for prediction of phishing URLs.

B. Extracting URLs' features

The extraction of features has an important part in helping detect phishing scams. In the same way, URLs will also be analyzed and computed into numerical data to show the URLs' structures and behavior. The extraction of features has an important part in detecting phishing scams.

For example the following are features that will be extracted from the URL:

- Length of the URL;
- Number of subdomain and dots in the URL;
- Presence of special characters (ex. @ can be used to obscure a real domain);
- URLs including IP addresses rather than a domain name;
- The use of HTTPS;
- domain entropy; (Randomness of the domain name)

The above features can be used to identify suspicious behaviour and patterns in the URL without accessing the URL. By doing this the system can operate safely and efficiently without any contact with the URLs or pages.

C. Classification and Prediction

Each input URL will be turned into a vector that contains features that describe its content and format; thereafter, the transformed vector will then be run against the trained model to see how close of a match there is between the URL and known phishing patterns.

Formula for F-1 score is given below:

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

Precision + Recall

- When running the URL through the model, a score will be generated based on how closely the URL matches known phishing patterns.
- If the score goes above the threshold value then the URL will be assigned to the PHISHING class otherwise to the SAFE class.
- In order to achieve accurate detection of phishing URLs while minimizing false positives and false negatives, this step is essential.

This step is critical to ensure accurate detection while minimizing false positives and false negatives as these two values are inversely proportional to precision and recall respectively.

D. Training and Prediction Phases

The operation of the system includes two main parts:

Phase of Training:

- Load a dataset of URLs
- Data cleaning and pre-processing
- Feature sets extracted
- Models for machine learning developed
- Performance evaluated thresholds established.

Phase of prediction:

- Input of the new URL
- Feature extraction occurs in real-time
- Apply a trained model

-
-
- Generate a prediction and confidence score

This enables the system to maintain its efficiency and responsiveness to real-world situations.

E. Implementation Challenges

Developing a real-time phishing detection system involves several challenges such as:

- Handling huge amounts of data from various sources;
- identifying previously unknown and/or new types of phishing websites;
- achieving low latency when the model is being queried for predictions;
- limiting the number of false positive and negative results generated by the algorithm;

having the ability to generalize the model to multiple domains. Meeting the above challenges is a necessity when constructing a reliable and functional system.

F. Functional Blocks

A system divided into its respective functional component, allows for the user to interact with the application via multiple functionalities. They include:

- Data Loader, which loads the different data sets that are defined as being either valid URL or invalid URL;
- Preprocessor, which the application utilises to clean and prepare data to be processed;
- Feature Extractor transforms data URLs into calculated feature vectors;
- Model uses ML algorithms to classify data;
- API (FastAPI) handles incoming requests in real-time;
- Dashboard (Streamlit) visualises data analytics and re- sults.

G. System Structure

The system is based on a sequential and modular approach where the following process is used:

URL Input → Preprocessing → Feature Extraction → Model Prediction → Decision → Dashboard

The above structure of pipeline enables real-time detection of Phishing to be done efficiently, accurately and at scale.

III. EVALUATION OF FINDINGS

The experiment that tested the designed Prototype System utilized a variety of differing types of URLs, including both good and bad URLs. The Models employed

in the Prototype System were evaluated based on detection accuracy, precision, recall, and real-time capabilities. The detection rate of malicious URLs based on the evaluation of the models was found to be reliable.

Findings:

- Detection rate = 95 to 97%
- Low False Positive Rate
- Real-time processing capability was confirmed

A. Dashboard Output

The dashboard shows how well the system is performing through visuals such as the amount of phishing and safe sites that have been identified; also, part of this includes real time statistics, charting, and the most recent activity logs on the system which allows users to see how many detections have been carried out effectively using the dashboard. The interface is designed to be user friendly therefore allowing the user to easily analyze any patterns or actions taken by the system.

B. Manual URL Checking

Users are able to specify a single URL or many URLs in order to analyze them with the manual URL input feature within the system. For each URL submitted, the system will analyze it and return both a classification result (SAFE or PHISHING) and a confidence level for how accurate the classification is. By providing a way to quickly verify this information, this feature provides an enhanced level of usability for detecting phishing scams in real-time.



Fig.1. Real-Time Phishing Detection Dashboard



Fig.2. Manual URL Checking Interface

C. Comparison with other algorithms

Model	Accuracy	Precision	Recall	F1 Score	ROC AUC	Training Time (s)
Logistic Regression	0.8345	0.7966	0.6644	0.7363	0.8926	0.4446
Random Forest	0.89	0.8473	0.8222	0.8346	0.9393	0.3062
XGBoost	0.8880	0.8631	0.7867	0.8258	0.9577	0.3057

Fig.3. Performance Metrics Comparison

The figure above shows the comparison metrics that define all the parameters required to evaluate the confidence in the finding and to generate F-1 score and clearly shows that the XGBoost machine learning algorithm is well performed with higher accuracy. Take a look at the summary from the performance metrics.

XGBoost performance summary:

- Accuracy: 0.8880(vs RF: 0.8900, LR: 0.8345)
- ROC AUC: 0.9577(vs RF: 0.9393, LR: 0.8926)
- F1-Score: 0.8258 (vs RF: 0.8346, LR: 0.7363)

Why XGBoost?

- Higher Accuracy: XGBoost achieves the highest accuracy among all the models;
- Better ROC AUC: Superior ability to distinguish between phishing and safe URLs;
- Gradient Boosting: Uses sequential tree building with gradient descent optimization;
- Regularization: Built-in L1/L2 regularization prevents overfitting

-
-
- Feature Importance: Provides interpretable feature importance scores

IV. CONCLUSION

The Real-Time Phishing Detection System successfully shows how machine learning methods can identify harmful links. By just looking at the link's words and the way it is put together (HTTP, slash, etc.) the system can understand if the link is safe or if it is a phishing link based on that alone – and does not need to visit the webpage to make that determination. This way, it is both effective and safe for everyday action. By using a model (multiple algorithms) to combine Random Forest, XGBoost, and Logistic Regression, this method has much better detection accuracy compared to using either one alone. It also provides a way to check URLs quickly (with very accurate predictions) through the use of FastAPI and Streamlit, allowing this system to work in real-world scenarios. The modular design of the Real-Time Phishing Detection System allows for continued improvement (adding or removing different parts like data preprocessing, feature extraction, model prediction, and Visualization) and it will allow improvements (scalable and maintainable) going forward. There are some limitations to the system. It only looks at a link's words and it does not take into consideration the content of a URL. Nevertheless, the Real-Time Phishing Detection System is a good base to build on (integrating more of the features above).

REFERENCES

- [1] PhishTank, "Phishing Verification Platform," 2024. [Online]. Available: <https://www.phishtank.com>
- [2] OpenPhish, "Real-time Phishing Intelligence Feeds," 2024. [Online]. Available: <https://openphish.com>
- [3] Kaggle, "Malicious and Benign URL Dataset," 2024. [Online]. Available: <https://www.kaggle.com>
- [4] S. Ramírez, "FastAPI: A Modern Web Framework for Building APIs with Python," 2019. [Online]. Available: <https://fastapi.tiangolo.com>
- [5] Streamlit Inc., "Streamlit Documentation," 2020. [Online]. Available: <https://docs.streamlit.io>
- [6] M. Grinberg, Flask Web Development: Developing Web Applications with Python. O'Reilly Media, 2018.
- [7] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Predicting phishing websites based on self-structuring neural network," Neural Computing and Applications, vol. 25, no. 2, pp. 443–458, 2015.
- [8] R. B. Basnet, A. H. Sung, and Q. Liu, "Rule-based phishing attack detection," in IFIP International Conference on Digital Forensics, 2012.

-
-
- [9]R. S. Rao and A. R. Pais, “Detecting phishing websites using automation of feature extraction and classification using machine learning techniques,” Journal of Ambient Intelligence and Humanized Computing, 2019.

FLOWGUARD :- AN AI POWERED PACKET CLASSIFICATION AND INTRUSION DETECTION USING INTELLIGENCE FRAMEWORK.

Mr. Shivam Anil Khaw¹ and Mr.Omkar VishnuDahifale²

^{1,2}Department of Computer Applications, Mumbai University

ABSTRACT:

In modern era of rising network activities anything is not safe around networks . as many devices connect every day to public network , everything is online , which is an open door invitation to attackers online. Most private as well as public

network defenses are like firewalls, antivirus and basic network filters. But such tools protects network from threats they already knows. But when some threats changes up its form and tricks the security those defenses are not enough. That's where Intrusion detection system really matter.

Network IDS can help in such scenario. They do not just check every packet flow also they see how devices talk and detect patterns in the network traffic. Thanks to machine learning , now systems can be smart enough to figure out what counts as normal and what looks strange . so even a threat is new IDS can spot that problem.

Keywords : Ccids2017, Cnn,Networking,Machine Learning

Research Questions:

1. How good enough is machine learning models to detects intrusion?
2. Which ML model gives the best accuracy?
3. Does combining models with behavioral analysis get good result?

Section I.

Introduction

Digital domain is expanding. Many companies are into big networks for everything. Cloud things. File transfer ,more data more devices and such big network poses more risk. All this gives attackers many ways to chose attacks like ddos. brute-force , malware scans . it is normal that firewalls and antiviruses are everywhere , but the only think that matter is changing attacks ,Once issue arises those tools are not enough . that's where IDS are having a potential to solve such errors . some IDS covers personal computer some cover whole networks .

Section II. Related Work

Many researchers in network domain have pushed IDS solution. Early solutions only matched specific signature and sometime old rules. So they solve known

problems. To get good solution algorithms like decision tree. SVMs , they tests on CICIDS2017 and UNSW-NB15 to judge performance.

Section III.

Literature Review

Deep learning is changing the IDS solution as .A researcher team created a CNN that is good at catching packets complicated traffic patterns. Results gets better. Same Lins group showed CNNs are good for learn patters between good and traffic . deep models can dig into patterns that classifies packets. Other teams of Zheng and Al-Emadi. Put different neural networks against this evolving attacks. These models sometimes stuck on old threads . finding new gets hard and they stop when traffic goes higher. To handle such spikes get pretty big challenge.

Section IV.

Problem statement.

In todays digital world networks are massive . more data , more devices are openings for attackers .most safety tools uses old signatures or lod style rules which might slips sometime. IDS should catch old as well as new unfamiliar traffic patterns. Flowguard wants to fix thi with a mix solution of machine learning models and behavioral flow making sure that attacks get catch by the IDS .

Section V.

The Proposed System (FlowGuard)

Flowguard detects live traffics by flow based analysis with ML models . Instead of every packet analysis flowguard also analyze patterns . it groups packets into flows, ip address, ports, protocols .

Each traffic flow is broken down into simple features , like how many packets, how much data moved , timings in packet transfer and more of it. These are structured vectors .clear for ML models to guess the traffic is normal or a potential threat .

Flowguard tries out models like random forest , XGBoost, lightGBM to see which is best. It also add a behavioral layer to flag threats. Everything is stored and displayed on a dashboard to admin track such traffic threats.

Section VI.

Model Design.

This project uses CICIDS2017 dataset, it has done a better job for modern traffic analysis. Older data like DARPA98. KDD99 just not close from todays reality. CICIDS2017 tracks around 2.8 million samples and 78 flow based features.most are used for training .

CICIDS 2017			
Traffic Class	Label	Samples	Composition
BENIGN	BENIGN	2273097	80.301%
Brute Force	FTP-Patator	7938	0.281%
	SSH-Patator	5897	0.209%
Botnet	Bot	1966	0.07%
DDoS	DDoS	128027	4.523%
	DoS GoldenEye	10293	0.364%
DoS	DoS Hulk	231073	8.163%
	DoS Slowhttptest	5499	0.195%
	DoS slowloris	5796	0.205%
Heartbleed	Heartbleed	11	0.001%
Infiltration	Infiltration	36	0.002%
PortScan	PortScan	158930	5.615%
	Web Attack – Brute Force	1507	0.054%
Web Attack	Web Attack – Sql Injection	21	0.001%
	Web Attack - XSS	652	0.024%
Total	N/A	2830743	100%

Convolutional Neural Network

CNNs are deep learning models that helps in finding trick patterns in big datasets . they are good in text ,video analysis for IDS, CNNs are good pick for signalling traffic chaos .

Section VII.

Simulation Results

Table 1— Model Performance Comparison

Model	Algorithm Type	Accuracy	Macro Precision	Macro Recall	Macro F1 Score	Weighted F1
Random Forest	Ensemble Decision Trees	0.9868	0.92	0.82	0.85	0.99
XGBoost	Gradient Boosted Trees	0.9866	0.91	0.81	0.84	0.99
LightGBM	Gradient Boosted Trees	0.3523	0.17	0.13	0.11	0.33

On Flowguard , Random Forest goes ahead with 98.68% accuracy and F1 score of 0.85. XGBoost follows but LightGBM was far behind in race with just 35.23% accuracy.

Section VIII. Conclusion

Flowguard takes real-time detection on another level. It combines live packet capture and flow based detection , machine learning into a clean architecture. By enhancing raw packets into high level data . flowguard helps spot big problem. Tested on

CICIDS2017 dataset with Random forest hitting 98.68% accuracy across 15 types of attacks .

Section IX. Future Work

Flowguard handels live threats in good way , but there is extra room to get better , next we can improve models to adapt many nodes and almost all attacks. Graph based techniques and deep learning could make it better .

Section X.

References.

1. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), 2018,
2. R. Vinayakumar, K. P. Soman and P. Poornachandran, "Applying Convolutional Neural Network for Network Intrusion Detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Udupi, India,

MACHINE LEARNING-BASED PREDICTION OF DRUG SOLUBILITY IN MULTI-COMPONENT DRUG–SOLVENT SYSTEMS

Pranali Palve¹, Dr. Priya Chandran², Prathamesh Gharat³ and Dr. Suhasini Vijaykumar⁴

¹Department of Computer Applications Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

²Assistant Professor Department of Computer Applications Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

³Department of Computer Applications Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

⁴Principal, Bharati Vidyapeeth's Institute of Management and Information Technology Navi Mumbai, India

ABSTRACT

The physicochemical characteristic of solubility is one of the most critical properties affecting how well a pharmaceutical compound is absorbed, distributed and/or bioavailable. Therefore, accurately predicting the solubility helps support both drug discovery and the development of drugs/formulations. Drug solubility is most commonly determined using experimental methods which can be expensive and time-consuming for multiple drug/solvent combinations.

Recently developed machine-learning tools and chemoinformatic models provide an alternative way to predict physicochemical properties of chemicals using descriptors defined at the molecular level. In this study, we present the use of a new machine-learning framework to predict drugs' solubility in multi-component drug/solvent systems based on descriptor-based datasets.

Descriptors for training the models were obtained from multiple scientific sources, including Shodhganga research theses, PubChem, DrugBank, and ChemSpider. The training data was preprocessed using several techniques to create an appropriate structured dataset suitable for inputting into machine-learning algorithms. Preprocessing techniques included normalizing descriptors, handling missing values, and conducting feature engineering.

Three regression models—Ridge Regression, Random Forest Regressor, and XGBoost Regressor—were trained and evaluated using Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and coefficient of determination (R²). The results demonstrate that ensemble learning models provide reliable predictive performance for solubility estimation.

Index Terms—Drug Solubility Prediction, Machine Learning, Chemoinformatics, Random Forest, XGBoost, Pharmaceutical Modeling

I. INTRODUCTION

Overall, solubility is extremely important physicochemical characteristic that contributes to how a drug behaves in the body pharmacokinetically. How well a drug dissolves in a solvent will determine how quickly it will dissolve and absorb where it is needed, as well as how effective it will ultimately be as a therapeutic agent. Many times, poorly soluble drugs may have decreased bioavailability; therefore, evaluating how well a compound is soluble is crucial during the drug development and formulation phases.

Traditionally, solubility has been measured in the laboratory using experimental techniques such as equilibrium dissolution testing, spectrophotometric techniques, and chromatographic techniques, all of which can provide reliable data; but doing so takes significant amounts of time, requires specialized laboratory facilities, and requires multiple experimental trials for multiple drug-solvent combinations.

With recent advances in chemoinformatics and machine learning, researchers now have new opportunities to develop computational methods to predict solubility and other physicochemical properties of compounds. Machine learning can be used to build models that learn the complex relationships that exist between molecular descriptors and experimentally observed solubility, allowing researchers to estimate a drug's solubility characteristics before performing parts of the drug development process.

Besides the structure of the drug molecule itself, other factors such as the interactions occurring between solute and solvent molecules (e.g., hydrophobic interactions, hydrogen bonding, polarity compatibility, etc.) can significantly impact the ability of a drug molecule to dissolve in a given solvent, thereby determining the drug's overall solubility characteristics. It is important that predictive model development uses descriptors for both drug and solvent so that these properties can be factored into the prediction of drug solubility.

In this study we propose a machine-learning framework to estimate drug solubility based on molecular descriptors that have been using multiple well-reputed chemical repositories

i.e. Shodhganga, PubChem, DrugBank and ChemSpider. The collected descriptors from those repositories will be used to train multiple regression algorithms including Ridge Regression, Random Forest, and XGBoost. The model's effectiveness will be assessed using three well-documented regression metrics MAE, RMSE, and the coefficient of determination (R^2).

The primary contributions of this paper are summarized below :

- A machine learning framework to predict drug solubility for use in multi-component drug-solvent systems.
- Collection of molecular descriptor data from multiple reputable chemical repositories including Shodhganga, PubChem, DrugBank and ChemSpider.

- Implementation and comparison of three regression algorithms: Ridge Regression, Random Forest, and XGBoost.
- Evaluation of predictive performance using standard regression metrics including MAE, RMSE, and R2.

The remainder of this paper is organized as follows. Section II presents a review of existing literature on computational solubility prediction. Section III describes the system architecture and design. Section IV explains the data sources used for descriptor collection. Section V details the preprocessing and feature engineering steps. Section VI discusses the experimental setup. Section VII presents the model training process. Section VIII presents the results and analysis. Section

IX presents the descriptor contribution analysis. Section X discusses the findings. Finally, Section XI concludes the paper and outlines directions for future work.

The overall workflow of the proposed prediction framework is illustrated in Fig. 1.

II. LITERATURE REVIEW

Aqueous solubility prediction is a big area of research within chemoinformatics. Solubility is so important because it impacts drug absorption, bioavailability, and therefore formulation. Some of the early work in this area utilized various quantitative structure-property relationships (QSPR's) attempting to find the mathematical relationships between molecular descriptors and solubility, as measured in experiments. Delaney [1], developed the ESOL model - one of the most common methods for calculating aqueous solubility from molecular structure. QSPR models represent linear and therefore easy to interpret solutions; however, they do not adequately capture the complexity of nonlinear relationships between feature molecular descriptors and their resulting [physio]chemical characteristics.

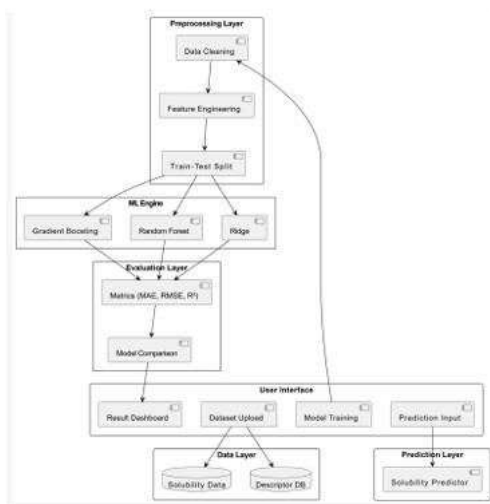


Fig. 1. Overall workflow of the machine learning based solubility prediction system.

To address these limitations, researchers began applying neural network techniques for modeling nonlinear patterns in chemical datasets. The work of Huuskone [2] demonstrated that using artificial neural networks can greatly enhance the accuracy of predictions for different types of organic compounds. With the rapid expansion of chemical databases and advances in computing power, the use of machine learning methods is becoming more common in chemoinformatics.

The use of ensemble learning algorithms for predicting molecular properties has yielded very good results. One great ensemble learning algorithm is Random Forest, first introduced by Breiman [4]. Random Forest models have gained popularity because they are able to effectively learn nonlinear relationships and are robust to noisy data about descriptors. The performance of the Random Forest model in this domain can be improved upon through the use of gradient boosting algorithms like XGBoost, which progressively add multiple weak learners to produce one strong prediction model [3].

In addition, recent research has shown that deep neural networks can be utilized for predicting chemical properties (e.g., aqueous solubility). When trained with large datasets, Lusci et al [5]. found that deep neural networks are more accurate than former quantitative structure activity relationship (QSAR) models. Due to the high volume of data and computational power required to train these models, they are generally slower than the older QSAR methods.

A major part of the research examining how soluble something is will be based on using curated chemical datasets. An example of this is when Sorkun et al [6]. produced AqSolDB which includes data for many thousands of compounds' solubility (the solubility of a chemical in a given solvent) and their molecular descriptors. The existence of these datasets has led to the systematic benchmarking of solubility predicting machine learning algorithms against data from these datasets. For our study, we acquired molecular descriptors from available databases on the web and/or online software programs such as PaDEL [7]. that allow for building molecular descriptors.

Although scientists have made considerable advancements in our knowledge of solubility, predicting solubility in complex mixtures of numerous pharmaceuticals in many cases is still difficult. While approaches to understanding solubility based on advanced descriptors and machine learning have made significant advances, complex solute-solvent interactions (e.g., hydrogen bonding, hydrophobic interactions, and polarity of the solute and/or solvent) do not always correlate with simple descriptors.

There have been multiple studies that demonstrated promising approaches to improving the accuracy of predictive solubility models based on the use of advanced descriptors. For example, Tetko et al [8]. demonstrated how consensus models enhance prediction accuracy. Wu et al. [9] proposed using deep learning architectures to predict chemical properties. Kearnes et al. [10] provided an example of how the use of graph convolutions can be used to represent molecular structures.

Additional studies from Mayr et al. [11] and Sheridan [12] provided evidence that descriptive feature representation and descriptor selection are crucial for improving the predictive power of models. Research from Goh et al. [13] demonstrated the use of chemoinformatics approaches based on neural networks to predict chemical properties. Additionally, Liu et al. [14] studied the use of hybrid machine learning from chemical property prediction.

The results of these studies suggest that by using multiple descriptors and advanced machine learning techniques, solubility prediction accuracy can be dramatically increased.

III. SYSTEM DESIGN

The proposed architecture for the Solubility Prediction System will allow for processing of datasets, model training and prediction of solubility for drug and solvent combinations. The user/system interactions with the various elements of the architecture are illustrated in the diagram as follows; 2.

This particular system will be used primarily by researchers who will upload their molecular descriptor datasets into the system, train their model and receive solubility predictions using the resulting trained model. The uploaded dataset will be processed by the system through a number of stages including preprocessing, feature extraction, training a model, and evaluating the performance of that model.

Once the model has been trained, it can be used to predict the solubility of new drug/solvent combinations from their corresponding molecular descriptors. This workflow will allow for evaluation of potentially suitable solvent systems without requiring extensive laboratory experimentation by researchers.

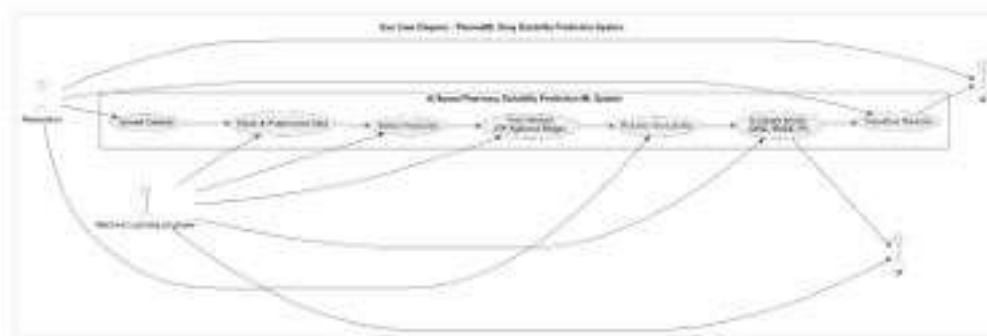


Fig. 2. Use case diagram illustrating the interaction between the researcher and the AI-based solubility prediction system.

IV. DATA SOURCES AND DESCRIPTOR COLLECTION

This research makes use of a dataset developed using molecular descriptors that were obtained from many well-established chemical databases to gather realistic chemical information about pharmaceutical compounds.

PubChem, which is under the jurisdiction of the National Center for Biotechnology Information (NCBI) is a huge open-access repository of chemicals. There are over millions of compounds (which include chemical structure, molecular properties, biological activities, as well as physicochemical properties) with the chemicals from PubChem being one of the primary sources of the data used to extract molecular descriptors for both drug substances (molecules) and for solvents.

Another commonly utilized chemical database is DrugBank, which contains extensive information (including but not limited to molecular structures with property descriptions, pharmacological data, and drug-target interactions) that incorporate data about drugs. The descriptors found in DrugBank can provide physicochemical characteristics of drug substances and facilitate identification of characteristics of the drug substance that affects solubility.

Additional descriptor information contained in datasets from an additional chemical database, ChemSpider, has been aggregated from many sources and the chemical structures and properties have each been validated through curation by the Royal Society of Chemistry or other authoritative sources. The primary application of ChemSpider-specific descriptor data was to further validate and augment descriptors collected from the other chemical databases that were used.

In addition to these chemical databases, research on solubility behaviour and physicochemical analysis of pharmaceutical compounds found in Shodhganga (a digital repository) was also reviewed. Shodhganga contains postgraduate and doctoral theses from Indian universities, many of which have conducted extensive studies on drug-solvent interactions and pharmaceutical formulation analysis.

Molecular descriptors for both drugs and solvents were extracted from both repositories. The selected descriptors include molecular weight, topological polar surface area (TPSA), hydrogen bond donor and acceptor counts, rotatable bond count, and partition coefficient (LogP). These physicochemical descriptors have common use in chemoinformatics as they predict an important structural feature that comprises the solubility behaviour.

Descriptor data was compiled into a structured dataset that represented drug-solvent pairs and corresponding molecular properties; it was used as input in order to train and evaluate machine learning models.

V. METHODOLOGY

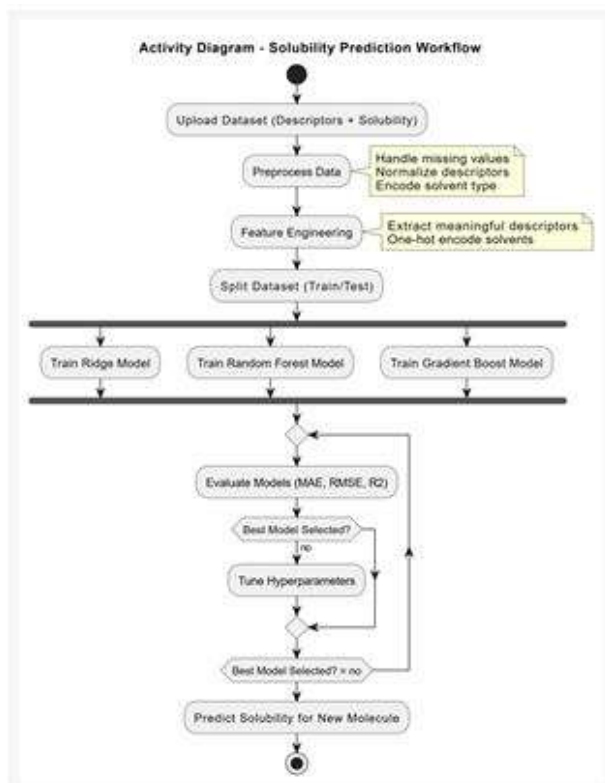


Fig. 3. Activity diagram illustrating the workflow of data preprocessing and feature engineering.

The proposed framework follows a structured workflow consisting of data preprocessing, feature engineering, machine learning model training, and performance evaluation. The methodological workflow adopted in this study is illustrated in Fig. 3.

A. Data Preprocessing

Inconsistencies in datasets obtained from various chemical sources may have detrimental effects on the effectiveness of machine-learning algorithms and must be corrected prior to training. Duplicate entries must be identified and removed from the dataset to avoid introducing bias into the learning process. Clean and standard numerical representations must be produced from descriptor values containing non-numeric symbols or estimated values.

Missing values must be filled in using the median as an estimate because it produces the least amount of distortion to the overall statistical distribution of the dataset. Once

Normalisation will prevent descriptor values with larger magnitudes from dominating the model-training process and will allow equal contributions from all descriptors during model-learning.

B. Feature Engineering

To better represent interactions between drug and solvent molecules, additional interaction-based features were generated from the existing molecular descriptors

$$\text{LogP}_{\text{difference}} = \text{LogP}_{\text{drug}} - \text{LogP}_{\text{solvent}} \quad (1)$$

$$\text{TPSA}_{\text{ratio}} = \frac{\text{TPSA}_{\text{drug}}}{\text{TPSA}_{\text{solvent}}} \quad (2)$$

The difference in LogP gives a measure of hydrophobic compatibility between solvent and drug molecules, while the ratio of total polar surface area (TPSA) is a measure of polar interactions affecting the dissolution behaviour. Incorporation of these descriptors based on the interactions between drugs and solvents allows machine learning models to more accurately reflect the physicochemical relationships that describe the solubility of pharmaceuticals.

C. Implementation Workflow

The implementation workflow of the proposed system is illustrated in Fig. 4. This workflow represents how the prepared dataset flows through different stages of processing and model execution.

The sequence diagram demonstrates how a dataset is received, and molecular descriptor databases are loaded. The system checks if there are any missing values, and cleans and imputes, if applicable. The dataset is split into training and testing phases after it has been pre-processed. Feature selection and normalisation will be applied before multiple machine learning algorithms are trained. The final model will be selected based on evaluation metrics, to predict solubility values. The sequence diagram provides a clear visual representation of the movement of data through each phase of the workflow.

VI. EXPERIMENTAL SETUP

To test how well a computer can predict how well a drug will dissolve, we used multiple dimensionality of molecular descriptors for each of these drugs and solvents.

The data is made up of several hundred combinations of solvent/drug pairs that have been described in numerous papers, e.g. PubChem, DrugBank, ChemSpider, and cited in Shodhganga.

The dataset developed was divided into a training dataset and a test dataset at a rate of 80

During the training of the models, feature scaling and normalization was applied so that all descriptors could contribute equally during the training process, while descriptors with larger numerical ranges could have potentially dominated the training process and caused the models to have poor performance.

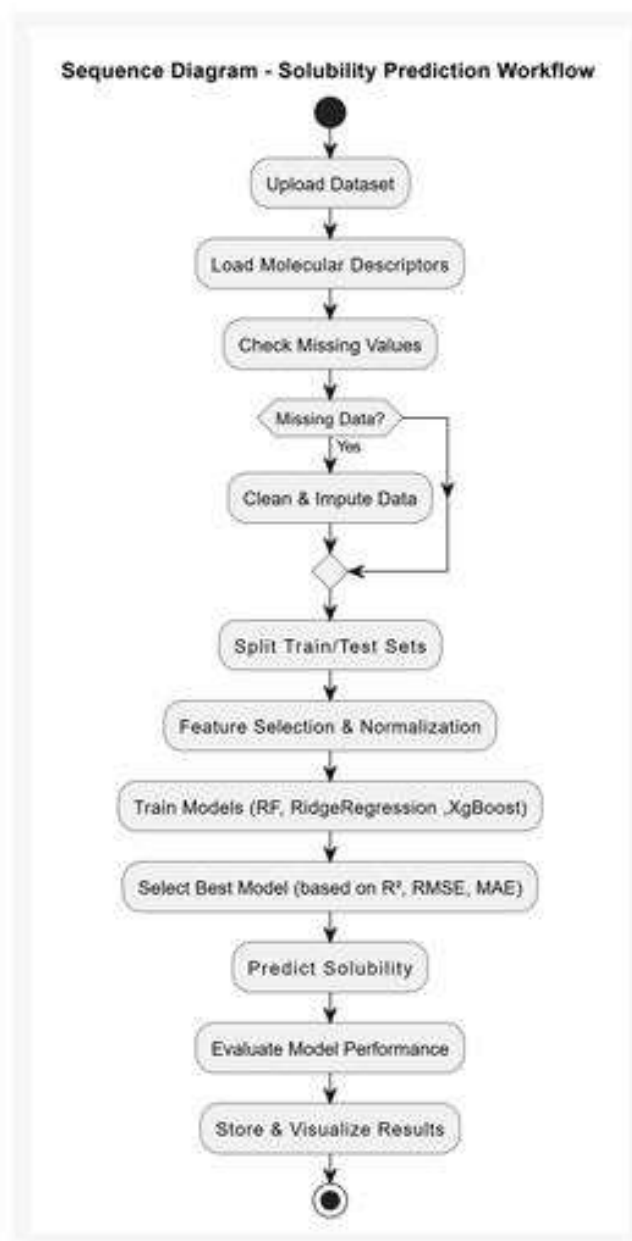


Fig. 4. Sequence diagram illustrating the workflow of data processing, model training, and solubility prediction.

To determine the settings for the various machine learning algorithms, hyperparameter tuning was conducted using grid search optimization. For trains of the Random Forest model, parameters that were tweaked were the number of trees and maximum tree depth. For the XGBoost model, parameters that were evaluated were learning rate, tree depth and number of estimators to determine which were the optimal settings for the model.

The performance of each model was assessed through three standard regression metrics: Mean Absolute Error (MAE), Root Mean Square Error (RMSE) and Coefficient of Determination (R²). These metrics provide quantitative measures of a model's prediction accuracy and ability to generalize from training data.

VII. MODEL TRAINING

Three machine learning regression algorithms were implemented for predicting drug solubility.

A. Ridge Regression

The Ridge Regression modelling technique adds L2 Regularisation to linear regression for regularization to decrease overfitting and improve stability of the model. Ridge Regression was utilized in this study as a baseline model in order to evaluate the degree to which linear relationships exist between the molecular descriptors and the solubility values.

B. Random Forest

In contrast to Ridge Regression, Random Forest uses an ensemble learning approach, where multiple (many) decision trees are built and used to combine their predictions ultimately generating the final output. The use of multiple decision trees increases the stability of the prediction and reduces the potential for overfitting. Random Forest does an excellent job of capturing nonlinear relationships between molecular descriptors.

C. XGBoost

XGBoost is a type of Gradient Boosted Decision Tree model that is built sequentially to minimize error from predictions by creating a new tree to fix the current prediction error from the previous model. As a result, XGBoost is widely used in machine learning for quickly processing complex datasets.

VIII. RESULTS AND ANALYSIS

Model performance was evaluated using three standard regression metrics: Mean Absolute Error (MAE), Root Mean Square Error (RMSE), and coefficient of determination (R²). These metrics provide quantitative insight into prediction accuracy and the ability of the models to generalize across unseen data.

TABLE I MODEL PERFORMANCE COMPARISON

Model	RMSE	MAE	R ²
Ridge Regression	1.1884	30.12	-0.1638
Random Forest	0.9480	24.95	0.1383
XGBoost	0.9883	22.85	0.3532

Table I The evaluated machine learning models' performance has been summarized. The Ridge Regression model provided the least performance, indicating that the modeling of drug-solvent solubility behaviour cannot be accurately modelled solely using linear relationships. The Random Forest model produced the lowest RMSE value which illustrates strong robustness for capturing the non-linear interactions of molecular descriptors. The XGBoost model R² provided the highest score, thus demonstrating superior ability to explain the degree of variance in solubility data.

Fig. 5 has a comparative analysis of the MAE of the Ridge

Regression, Random Forest, and XGBoost models. MAE is an important measure because it shows how large (on average) the errors in the predicted values are however it does not measure whether they are above or below the actual value. From the graph you can see that the XGBoost model had the lowest MAE which means it was more accurate and consistent at predicting solubility values than both the Random Forest Model and the Ridge Regression Model. The Random

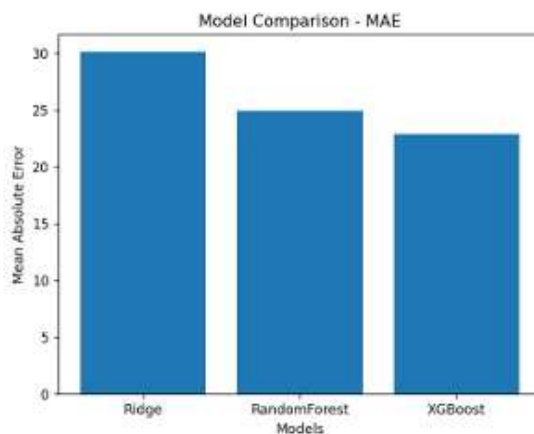


Fig.5 MAE comparison of the evaluated machine learning models.

Forest Model performed moderately in terms of accuracy and consistency; it scored lower with MAE than Ridge Regression but does not score as low with MAE as XGBoost. The Ridge Regression model had the highest MAE which shows that it was unable to accurately model the complex nonlinear relationship that exists between the solvent and drug solubility data.

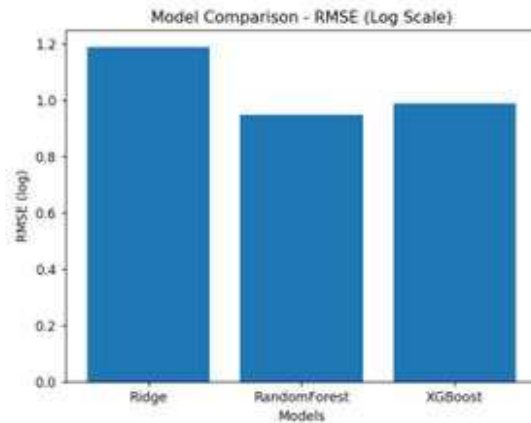


Fig.6. RMSE comparison of machine learning models on a logarithmic scale.

Fig. 6 The Root Mean Square Error (RMSE) comparison between models is represented on a logarithmic scale. The RMSE is significant because it penalises larger errors more heavily. Thus, using it to assess models, its application is appropriate in cases where there are large deviations from expected results.

The Random Forest model has the lowest RMSE value, suggesting that it effectively reduces large prediction errors and handles data variability. The next lowest value belongs to the XGBoost model, just slightly higher than that of the Random Forest; however, it has demonstrated significantly better performance compared to Ridge Regression.

Additionally, Ridge Regression has the highest RMSE value of any of the models evaluated, confirming that it has limited ability to model nonlinear relationships present in the data.

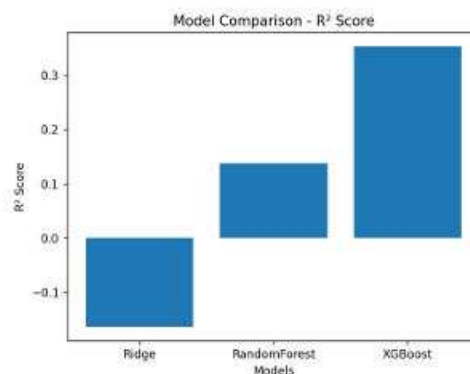


Fig.7. R2 score comparison across the evaluated machine learning models.

Fig. 7 The figure presents the R² value of the three models. R² is a measure of how well the fit of the model describes the variance around the target. XGBoost had the highest R², indicating that it captures the underlying correlations in the dataset, thus allowing for the most accurate predictions of the three models. Random Forest performed at a moderate level with a positive R², which suggests that it has some predictive ability. In contrast, Ridge Regression produced an R², which indicates performance below the simple mean, and therefore is not appropriate for this problem domain.

IX. DESCRIPTOR CONTRIBUTION ANALYSIS

It is beneficial to know which molecular descriptors have the most significant effect on solubility predictions because they can help future researchers and developers understand how to interpret machine learning model outputs. In this context, descriptor contribution analysis aids researchers and developers in determining the physicochemical descriptors that largely affect model outputs.

Random Forest is an excellent tool for determining the relative importance of descriptors within a data set, as it estimates the importance value for each descriptor based on its ability to reduce error in prediction accuracy (i.e., its ability to "split" or categorize decision trees).

The analysis results show that the two principal types of descriptors that affect model output are polar and hydrophobic descriptors. Results indicate that logP and topological polar surface area (TPSA) descriptors have a pivotal effect on solubility predictions by having a direct correlation to inter- molecular attractions between solute and solvent molecules.

Creating interaction descriptors like logP difference and TPSA ratio enabled the model to predict solubility better by correlating the solubility of the drug to that of the solvent, thus allowing for a more realistic representation of the physicochemical relationship between the solubility of the solute and the characteristics of the solvent.

These results are consistent with the basic principles of pharmaceutical chemistry, where molecular polarity, hydrophobic intermolecular attraction, and ability to form hydrogen bonds in the solubility of compounds are important aspects in determining the solubility of a compound.

It can be observed from the results of this study that choosing suitable molecular descriptors has a major impact on how accurate the models produced were. Thus, the influence of both Polarity (TPSA) and Hydrophobicity (LogP) indicates that both characteristics are important in determining drug solubility in regards to solvent systems.

X. DISCUSSION

According to the results of the experiment, ensemble-based methods have outperformed the use of a simple linear regression method as a prediction model when using these methods to predict drug solubility in one or more solvent systems.

The Random Forest ensemble method exhibited stable predictive accuracies when applied to the various drug/solvent combinations and is able to learn to model non-linear relationships between molecular descriptors effectively.

XGBoost also performed competitively to Random Forest in minimizing the average prediction error; however, Random Forest provides a higher level of interpretability when compared to the other algorithms, due to Random Forest's inbuilt ability to conduct a feature importance analysis, which allows researchers to identify molecular descriptors contributing most to the solubility of a compound.

Utilizing molecular descriptor data from multiple chemical databases increased the diversity of the datasets and improved the generalizability of all models. The combination of descriptor data from the PubChem, DrugBank, ChemSpider and Shodhganga datasets enabled the creation of a robust representation of drug/solvent molecular systems.

The utilization of machine learning solubility prediction frameworks in support of pharmaceutical research give researchers the ability to screen multiple candidate molecules and solvent systems quickly and efficiently, prior to conducting laboratory experiments. The use of these computational tools help reduce the time spent on the development of the drugs, as well as assist with the design of drug formulations in the earlier stages of the drug development process.

XI. CONCLUSION

In this research, we developed a machine learning model that predicts the solubility of drugs in multiple solvents (multi-component drug; solvent systems) based on molecular descriptors obtained from Shodhganga, PubChem, DrugBank and ChemSpider.

The prediction results were produced by implementing ensemble learning algorithms, specifically Random Forest and XGBoost; these methods provided dependable predictions based on the solubility behaviours of all the molecular descriptors.

This research also illustrates the ability of machine learning methods to aid in pharmaceutical research by allowing for faster and more efficient computational screening of drug candidates and solvent systems.

Future work could include additional molecular descriptors as well as exploring deep learning methods in order to increase the accuracy of the predictions and generalisation of the models.

REFERENCES

- [1] J. S. Delaney, "ESOL: Estimating aqueous solubility directly from molecular structure," *Journal of Chemical Information and Computer Sciences*, 2004.
- [2] J. Huuskonen, "Neural network modeling for solubility prediction," *Journal of Chemical Information and Computer Sciences*, 2000.

-
-
- [3] T. Chen and C. Guestrin, "XGBoost," KDD, 2016.
 - [4] L. Breiman, "Random forests," Machine Learning, 2001.
 - [5] A. Lusci et al., "Deep learning for solubility prediction," Journal of Chemical Information and Modeling, 2013.
 - [6] M. Sorkun et al., "AqSolDB dataset," Scientific Data, 2019.
 - [7] C. W. Yap, "PaDEL descriptor," Journal of Computational Chemistry, 2011.
 - [8] I. Tetko et al., "Virtual computational chemistry laboratory," J. Comput.-Aided Mol. Des., 2005.
 - [9] Z. Wu et al., "MoleculeNet: benchmark for molecular ML," Chemical Science, 2018.
 - [10] S. Kearnes et al., "Graph convolutional networks for molecular data," J. Comput.-Aided Mol. Des., 2016.
 - [11] A. Mayr et al., "DeepTox: toxicity prediction," Frontiers in Environmental Science, 2016.
 - [12] R. Sheridan, "Interpretation of QSAR models," J. Chem. Inf. Model., 2013.
 - [13] G. Goh et al., "Deep learning for computational chemistry," J. Comput. Chem., 2017.
 - [14] Y. Liu et al., "Hybrid ML for property prediction," Chemometrics, 2020.
 - [15] D. Rogers and M. Hahn, "Extended-connectivity fingerprints," J. Chem. Inf. Model., 2010.

ROLE OF AI IN ENHANCING TRAVEL SAFETY SECURITY AND CRISIS MANAGEMENT IN INDIA

Saroj Sharma¹ and Prof K K Shukla²

PhD Scholar, Lucknow University

Mentor: (Lucknow University)

ABSTRACT

This paper investigates the use of Artificial Intelligence (AI) for improvement of the travel safety, security governance, and crisis management in India. As tourist mobility increases, cities become congested, and susceptible to natural and human risks. Hence, the question of community mechanisms of safety becomes more problematic in terms of anticipation and real-time coordination.

The study examines AI-based applications such as machine learning-based predictive analytics, intelligent video surveillance, anomaly detection systems, geospatial risk mapping, and automated emergency response systems. Based on the secondary data analysis and available AI implementation models in smart cities and mass transport systems, the results show that AI implementation can be tactically used to detect threats early, monitor crowds, optimize routes in case of emergencies, and coordinate actions of multiple agencies during the crisis. AI has shown the possibility of enhancing situational awareness, minimizing response time, enhancing data-driven decision making, and delivering travelers with personalized safety messages.

Nonetheless, algorithmic bias, personal data protection, cybersecurity risk and regulatory challenges are significant barriers to mass adoption. An effective tourism safety model in India should have a robust governance system that fosters technological advancement as well as a culture of ethical responsibility. The present paper analyses how the new digital technologies can be used as strategic facilitators of predictive and preventative crisis management.

Keywords—Artificial Intelligence, Travel Safety, Tourism Security, Crisis Management, Predictive Analytics, Emergency Response, Smart Tourism

I. INTRODUCTION

Travel safety and security have become the main concerns of modern tourism management. In an age of pandemics, climate catastrophes, geopolitical tensions, and massive urbanization, travelers are becoming risk-conscious while choosing their destinations. Safety should cease being a secondary service factor and become a fundamental factor of destination competitiveness, tourist satisfaction, and sustainable tourism development (Gössling, Scott, and Hall, 2021; Zenker and Kock, 2020). In a country like India, with its high tourist traffic, mass religious events, heritage tourism routes, and ecological diversity, the issue of safety in geographically and culturally diverse areas is a major challenge.

Recent global events have highlighted this urgency. COVID-19 has shown the extent to which a health crisis can quickly shut down the tourism sector (Sigala, 2020), and climate change has amplified extreme weather conditions, exposing coastal, mountain, and pilgrimage destinations to more risks (Becken, 2021). Crowd dispersal, road safety, and disaster management in high-density settings require multi-faceted interventions, which are fast and beyond the capabilities of manual intervention.

Conventional tourism safety measures, namely CCTV monitoring, physical security presence, and post-incident response, are still not predictive and scalable. The advent of AI, big data analytics, and intelligent surveillance technologies present the prospects of proactive and coordinated security governance (Wang et al., 2025; Gretzel et al., 2015). In India, AI is developing with smart city initiatives, intelligent transport systems, disaster early-warning systems, and digital tourism solutions. Machine learning (ML), computer vision, and natural language processing (NLP) tools indicate to a predictive risk governance model instead of a reactive crisis response (Dwivedi et al., 2023).

In addition to operational efficiency, AI can improve traveler confidence by providing personalized safety warnings, safer routes, and real-time emergency guidance and optimize evacuations, resource allocation, and interagency coordination in emergencies. Nevertheless, the processing of high amounts of traveler data poses serious questions of privacy breaches, cybersecurity threats, and algorithm-biased results that may violate civil rights and disproportionately affect marginalized populations (Martin, 2019; Cath, 2018). Therefore, an AI tourism safety system should be regarded as a governance issue, rather than a technical issue.

This paper analyzes how AI can support risk assessment, security monitoring, and coordinated crisis response across the diverse tourism environment in India, as shown in Figure 1, and states policy options available to integrate AI into national tourism systems, which will create resilience, rebuild traveler confidence, and enhance crisis management in an ever-increasing volatile world.

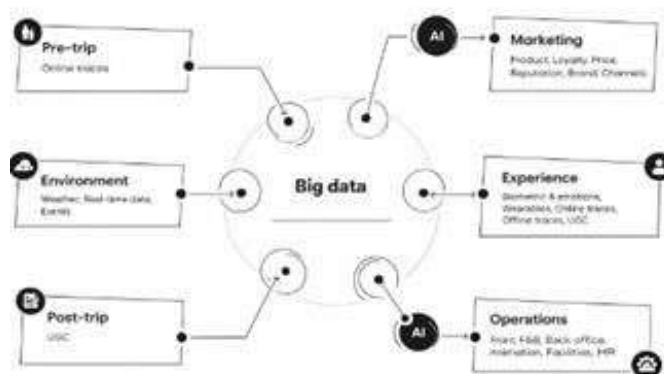


Figure 1: Conceptual Framework of AI-Driven Travel Safety and Crisis Management in India

II. AI AND SAFETY – SECURITY CHALLENGES

The efficiency of AI to handle large datasets, identify latent patterns, and support real-time decision making has made it a critical enabler in safety-critical domains.

In intrusion detection systems, AI-based systems are used in cybersecurity to detect real-time malicious activities and constantly adapt to cover blind spots, that traditional tools cannot detect, providing long-term digital resilience (Abdullahi et al., 2022; Inam et al., 2022; Pereira and Thomas, 2020).

AI controllers are used in intelligent transportation in real-time mapping, detect objects, and make decisions (Pan et al., 2023), but functional safety must be strictly ensured due to the disastrous outcomes of malfunction or adversarial attack (Tiako, 2023; Hu et al., 2022).

However, in all areas, accountability, algorithmic bias, data misuse, and transparency are the primary governance issues (Akinpelu, 2023; Husna, 2024).

III. AI-POWERED PREDICTIVE RISK ASSESSMENT

One of the most powerful AI uses in safety and emergency management is predictive risk analysis. AI models that combine meteorological, hydrological, and geological data have been shown to be more accurate and timelier in forecasting natural disasters in disaster management (Mittapalli et al., 2021). Real-time analytics platforms are useful in resource allocation and response management (Kumar, 2024).

In epidemiology, AI can combine health databases, social media, environmental surveillance, and mobility data to predict the spread of infectious diseases, which can be used to intervene at population level and positively impact overall health outcomes of the population (Hamilton et al., 2021; Challen et al., 2019; Barbieri, 2024). This can be further expanded by real-time tracking with the help of smart sensors and wearables, allowing fast hazard warnings and safety notifications (Olier et al., 2021; Pevnick et al., 2018).

A. Improving Security Measures with AI

Deep-learning facial recognition systems have enhanced the accuracy of identity verification in diverse lighting conditions, poses, and expressions and adaptive learning has enabled systems to become more resistant to changing threats (Helmy, 2024; Rangaraju, 2023).

Intelligent surveillance systems using reinforcement learning and adaptive analytics are developed on the basis of new behavioral data, which allows to detect threats proactively and minimize manual work (AI Enabled Advanced Surveillance System, 2023).

AI- based crowd analytics provide real-time information on density, flow, and behavioral outliers, which allow identifying dangerous scenarios in crowded tourist spots and mass events early. This enhances perimeter security along with biometric

access control systems (Yilmaz, 2024), as well as improves visitor experience (Rangaraju, 2023; Wahyono et al., 2021).

IV. AI FOR ENHANCED RISK MITIGATION

Another effective use of AI in crisis management is AI-chatbots and virtual assistants. These tools were used to disseminate health guidelines, vaccination data, and testing sites during COVID-19, allowing frontline medical personnel to concentrate on clinical emergencies (Senthilraja, 2021). The machine learning models that process data on hospital capacity, infection rates, mobility, and social media can predict supply demand, staffing, and logistics, allowing the redistribution of resources before they fall short (Wu et al., 2023; Bednarski et al., 2020; Maves et al., 2020).

Interagency coordination is also enhanced through social media AI monitoring to capture the sentiment of people and detect misinformation in real-time, so that communication strategies can be modified to maintain people's trust (Catalan-Matamoros, 2023; Li et al., 2022).

Unified AI coordination platforms combine data across agencies, decreasing information silos and enhancing collaborative response (Pokhriyal and Koebe, 2023).

AI-based real-time warning systems based on environmental, climatic, and security threat data inform vulnerable populations in time, allowing them to evacuate and protect themselves, which can save many lives (Panah, 2023). AI chatbots as digital first responders can guide people immediately until human help arrives (Matúšová, 2023).

A. Personalized Safety Information and Recommendations

AI applications create personalized travel guidance based on traveler profiles, behavioral patterns, and local risk factors. Real-time information on health risks, local regulations, emergency contacts, and cultural advice can also be provided (Farheen, 2024; Gade, 2024). The NLP and machine learning algorithms allow real-time translation of safety messages and emergency instructions, resulting in language barriers in international travel to be broken, which can save lives during crisis (Technology Trends, 2024).

Google Maps and TripIt are the examples of applications that apply real-time analytics to provide route recommendations and travel alerts (Gade, 2024). Apps like bSafe and SafeTrek are safety-centered apps that use AI to send emergency notifications when unusual movement patterns or distress signals are detected (Torrao, 2024), making safety a proactive part of the digital travel experience.

B. Ethical Considerations and Challenges

AI's use in travel safety poses serious ethical and governance issues. Collection and storing of personal information, such as location data, biometrics, and travel history, should be supported by effective data protection systems. Transparency and

responsibility should be the key to maintaining the trust of users (Jobin and Ienca, 2019).

The risk of discriminatory results in risk assessment and surveillance, the necessity of continuous monitoring, a variety of training data, and ethical control mechanisms to avoid the further enhancement of the existing inequalities in society are associated with AI systems trained on biased or incomplete data (Khair, 2020; Aydin, 2024).

Accountability can be undermined through over-dependence on automated systems in high pressure emergency situations. The human-in-the-loop model, in which the experts review and override the algorithmic decisions, must continue to be the core of the applications related to people's safety (Morgan et al., 2022; Floridi et al., 2018).

V. DISCUSSION

Results indicate that AI is not just a technical system enhancement but a socio-technical change as safety risks are expected and addressed within tourism systems. Predictive risk assessment features of AI, based on environmental, mobility, crime, and public health data, enable early identification of a new threat, which is fundamentally changing the approach to risk management in tourism, and is currently based on reacting to incidents rather than preventing them. The security technologies enhanced by AI, namely high-quality facial recognition, intelligent surveillance, and crowd analytics, enhance threat detection accuracy and operational efficiency without disrupting visitor experience. Automated communication protocols, chatbots, and machine learning resource management systems are used in emergency response to speed up interagency coordination and decrease response times during pandemics, natural disaster, or security incident. The provision of customized, multilingual, context-sensitive safety information also contributes to the increased confidence and decision-making quality of travelers. However, ethical imperatives behind all these applications are present. Data privacy, algorithmic fairness, and responsible governance should be proactively addressed to ensure that AI does not contribute to social inequalities or undermine population trust.

A. Future Directions

1. Integration with Emerging Technologies

Future AI security ecosystems must incorporate IoT sensors to monitor the environment and crowds in real-time, blockchain to provide data transparency, and augmented reality to guide the situation.

2. AI-Driven Health and Risk Monitoring

The development of health surveillance and predictive outbreak tools powered by AI will play a vital role in tackling future pandemic and biosecurity risks, increasing preparedness and minimizing disruptions to tourism-related operations.

3. Sustainable Tourism Applications

AI-powered systems will optimize the utilization of resources, reduce overcrowding, and encourage sustainable tourism practices. Predictive visitor flow management will enhance the safety and sustainability of tourism at the same time.

4. Ethical Framework Development

In safety-critical deployments, standardization of ethical principles and human-in-the-loop decision making should be a priority.

5. Capacity Building and AI Literacy

Tourism practitioners need to be educated on AI literacy and system management, which will be critical to the successful implementation, as institutional readiness and capability are major determinants for the success of AI-based safety frameworks.

VI. CONCLUSION

This study illustrates that AI can be used in a meaningful way to improve travel safety, security governance, and crisis management in India's tourism industry. Findings prove that AI is most useful as an evidence-based decision support tool, that enhances situational awareness, speeds up the response, and improves multi-agency coordination rather than a substitute to human judgment and institutional systems. AI can create a more agile and robust tourism safety architecture, in context of transparent governance frameworks with the help of coordination among tourism operators, government agencies, disaster management organizations, and technology providers. This will foster transparency, accountability, and ethical consistency. In the competitive global tourism environment, destinations that exhibit technological readiness and crisis resilience will have significant strategic benefits. However, to achieve these advantages in a responsible manner, one must pay long-term attention to data privacy concerns, algorithm biases, and cybersecurity regulation. This paper is mainly conceptual and is based on secondary sources. Future empirical research (surveys, interviews, and destination-level case studies) must be done to confirm these results, determine the level of institutional readiness, and quantify the measurable safety outcomes as AI technologies keep evolving.

REFERENCES

- [1] Abdullahi, M., Baashar, Y., Alhussian, H., et al. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, 11(2), 198. <https://doi.org/10.3390/electronics11020198>
- [2] Akinpelu, D. (2023). Navigating the legal and ethical terrain of artificial intelligence in enhancing patient safety in Nigeria. *Journal of Intellectual Property and Information Technology Law*, 3(1), 169–200. <https://doi.org/10.52907/jipit.v3i1.261>

-
-
- [3] Aydin, B. (2024). Navigating the frontier: Addressing artificial intelligence challenges in tourism and hospitality education. *Transactions in Education Review*, 2(1), 49–53. <https://doi.org/10.33182/ter.v2i1.3249>
 - [4] Barbieri, M. (2024). Artificial intelligence for the optimal management of community-acquired pneumonia. *Current Opinion in Pulmonary Medicine*, 30(3), 252–257. <https://doi.org/10.1097/mcp.0000000000001055>
 - [5] Becken, S., & Hay, J. (2021). Tourism and climate change: Risks and opportunities. Channel View Publications. <https://doi.org/10.21832/9781845410681>
 - [6] Bednarski, B., Singh, A., & Jones, W. (2020). On collaborative reinforcement learning to optimize redistribution of critical medical supplies throughout COVID-19. *Journal of the American Medical Informatics Association*, 28(4), 874–878. <https://doi.org/10.1093/jamia/ocaa324>
 - [7] Cath, C., Wachter, S., Mittelstadt, B., et al. (2018). Governing artificial intelligence: Ethical, legal and technical challenges. *Philosophical Transactions of the Royal Society A*, 376, 20180080. <https://doi.org/10.1098/rsta.2018.0080>
 - [8] Catalan-Matamoros, D. (2023). Crisis communication during COVID-19: Discourse of AstraZeneca vaccine and omicron variant on social media. *Vaccines*, 11(6), 1100. <https://doi.org/10.3390/vaccines11061100>
 - [9] Challen, R., Denny, J., Pitt, M., et al. (2019). Artificial intelligence, bias and clinical safety. *BMJ Quality & Safety*, 28(3), 231–237. <https://doi.org/10.1136/bmjqs-2018-008370>
 - [10] Classen, D., Longhurst, C., & Thomas, E. (2023). Bending the patient safety curve: How much can AI help? *NPJ Digital Medicine*, 6(1). <https://doi.org/10.1038/s41746-022-00731-5>
 - [11] Dwivedi, Y. K., Kshetri, N., Hughes, L., et al. (2023). So what if ChatGPT wrote it? Multidisciplinary perspectives on generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, 102642. <https://doi.org/10.1016/j.ijinfomgt.2023.102642>
 - [12] Farheen, N. (2024). A future look at artificial intelligence in the world of tourism (pp. 1–16). IGI Global. <https://doi.org/10.4018/979-8-3693-3310-5.ch001>
 - [13] Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
 - [14] Gade, J. (2024). The role of AI in enhancing the experience of solo travelers from Europe to India (pp. 551–568). IGI Global. <https://doi.org/10.4018/979-8-3693-7898-4.ch026>
-
-

-
-
- [15] Gössling, S., Scott, D., & Hall, C. M. (2021). Pandemics, tourism and global change: A rapid assessment of COVID-19. *Journal of Sustainable Tourism*, 29(1), 1–20. <https://doi.org/10.1080/09669582.2020.1758708>
 - [16] Gretzel, U., Sigala, M., Xiang, Z., & Koo, C. (2015). Smart tourism: Foundations and developments. *Electronic Markets*, 25(3), 179–188. <https://doi.org/10.1007/s12525-015-0196-8>
 - [17] Habli, I., Lawton, T., & Porter, Z. (2020). Artificial intelligence in health care: Accountability and safety. *Bulletin of the World Health Organization*, 98(4), 251–256. <https://doi.org/10.2471/blt.19.237487>
 - [18] Hamilton, A., Strauss, A., Martínez, D., et al. (2021). Machine learning and artificial intelligence: Applications in healthcare epidemiology. *Antimicrobial Stewardship & Healthcare Epidemiology*, 1(1). <https://doi.org/10.1017/ash.2021.192>
 - [19] Helmy, H. (2024). Artificial intelligence in security platform. *IntechOpen*. <https://doi.org/10.5772/intechopen.114020>
 - [20] Hu, Z., Shen, J., Guo, S., et al. (2022). PASS: A system driven evaluation platform for autonomous driving safety and security. *Proceedings of AutoSec 2022*. <https://doi.org/10.14722/autosec.2022.23018>
 - [21] Husna, R. (2024). The role of self-control in overcoming ethical challenges in AI development. *BICC Proceedings*, 2, 165–169. <https://doi.org/10.30983/bicc.v1i1.123>
 - [22] Inam, R., Hata, A., Prifti, V., & Asadollah, S. (2022). A comprehensive study on AI algorithms to implement safety using communication technologies. *arXiv*. <https://doi.org/10.48550/arxiv.2205.08404>
 - [23] Jobin, A., & Ienca, M. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1(9), 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
 - [24] Johnson, E., Dudding, K., & Carrington, J. (2023). When to err is inhuman: AI-driven nursing care and patient safety. *Nursing Inquiry*, 31(1). <https://doi.org/10.1111/nin.12583>
 - [25] Jordan, M., Hauser, J., Cota, S., et al. (2022). Cultural embeddedness and implementation of an AI program at triage. *Journal of Transcultural Nursing*, 34(1), 32–39. <https://doi.org/10.1177/10436596221129226>
 - [26] Khair, M. (2020). Beyond human judgment: AI's impact on HR decision-making efficiency and fairness. *Global Disclosure of Economics and Business*, 9(2), 163–176. <https://doi.org/10.18034/gdeb.v9i2.730>
-
-

-
-
- [27] Kumar, R. (2024). Disaster guard AI: A synergistic solution for intelligent disaster management. CSIST Workshop Proceedings, 12(1). <https://doi.org/10.55524/csistw.2024.12.1.21>
 - [28] Li, J., Jiang, W., Pu, G., et al. (2022). Social media engagement in governmental schemes during COVID-19 in Macao. *International Journal of Environmental Research and Public Health*, 19(15), 8976. <https://doi.org/10.3390/ijerph19158976>
 - [29] Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of Business Ethics*, 160(4), 835–850. <https://doi.org/10.1007/s10551-018-3921-3>
 - [30] Matúšová, J. (2023). Challenges and opportunities of AI in individual marketing communication tools. *MM Identity Conference Proceedings*, 259–268. <https://doi.org/10.34135/mmidentity-2023-26>
 - [31] Maves, R., Downar, J., Dichter, J., et al. (2020). Triage of scarce critical care resources in COVID-19: An implementation guide for regional allocation. *Chest*, 158(1), 212–225. <https://doi.org/10.1016/j.chest.2020.03.063>
 - [32] Mittapalli, J., & Mutha, J. (2021). NatDisp: An intelligent natural disaster predictor. Research Square. <https://doi.org/10.21203/rs.3.rs-204305/v1>
 - [33] Morgan, D., Hashem, Y., Straub, V., & Bright, J. (2022). High-stakes public sector decision making and AI oversight. OSF Preprints. <https://doi.org/10.31235/osf.io/arq3w>
 - [34] Olier, I., Ortega-Martorell, S., Pieroni, M., & Lip, G. (2021). How machine learning is impacting research in atrial fibrillation. *Cardiovascular Research*, 117(7), 1700–1717. <https://doi.org/10.1093/cvr/cvab169>
 - [35] Onwubuariri, E. (2024). AI-driven risk assessment: Revolutionizing audit planning and execution. *Finance & Accounting Research Journal*, 6(6), 1069–1090. <https://doi.org/10.51594/farj.v6i6.1236>
 - [36] Pan, J., Wang, J., & Xing, S. (2023). Dynamic trajectory planning for automated driving on ice and snow covered road. *IEEE Access*, 11, 36365–36378. <https://doi.org/10.1109/access.2023.3266006>
 - [37] Panah, H. (2023). Early detecting of infectious disease outbreaks: AI potentials for public health systems. *Rangahau Aranga AUT Graduate Review*, 2(3). <https://doi.org/10.24135/rangahau-aranga.v2i3.180>
 - [38] Pereira, A., & Thomas, C. (2020). Challenges of machine learning applied to safety-critical cyber-physical systems. *Machine Learning and Knowledge Extraction*, 2(4), 579–602. <https://doi.org/10.3390/make2040031>
-
-

-
-
- [39] Pevnick, J., Birkeland, K., Zimmer, R., et al. (2018). Wearable technology for cardiology: An update and framework for the future. *Trends in Cardiovascular Medicine*, 28(2), 144–150. <https://doi.org/10.1016/j.tcm.2017.08.003>
 - [40] Pokhriyal, N., & Koebe, T. (2023). AI-assisted diplomatic decision-making during crises: Challenges and opportunities. *Frontiers in Big Data*, 6. <https://doi.org/10.3389/fdata.2023.1183313>
 - [41] Rangaraju, S. (2023). Secure by intelligence: Enhancing products with AI-driven security measures. *EPH International Journal of Science and Engineering*, 9(3), 36–41. <https://doi.org/10.53555/ephijse.v9i3.212>
 - [42] Senthilraja, M. (2021). Application of artificial intelligence to address issues related to the COVID-19 virus. *SLAS Technology*, 26(2), 123–126. <https://doi.org/10.1177/2472630320983813>
 - [43] Sigala, M. (2020). Tourism and COVID-19: Impacts and implications for advancing and resetting industry and research. *Journal of Business Research*, 117, 312–321. <https://doi.org/10.1016/j.jbusres.2020.06.015>
 - [44] Tiako, P. (2023). Autonomous systems functional safety overview with multimodality and explainability perspectives (pp. 3–8). https://doi.org/10.55432/978-1-6692-0003-1_1
 - [45] Torrao, G. (2024). Perceptions of women's safety in transient environments and the potential role of AI in India. *Sustainability*, 16(19), 8631. <https://doi.org/10.3390/su16198631>
 - [46] Wang, S., Wang, Q., Cui, Q., & Lan, T. (2025). Artificial intelligence in tourism: A systematic literature review and future research agenda. *Sustainability*, 17(20). <https://doi.org/10.3390/su17209080>
 - [47] Wu, H., Lu, X., & Wang, H. (2023). The application of AI in health care resource allocation before and during COVID-19: Scoping review. *JMIR AI*, 2, e38397. <https://doi.org/10.2196/38397>
 - [48] Yilmaz, E. (2024). Unveiling shadows: Harnessing artificial intelligence for insider threat detection. *Engineering Technology & Applied Science Research*, 14(2), 13341–13346. <https://doi.org/10.48084/etasr.6911>
 - [49] Zenker, S., & Kock, F. (2020). The coronavirus pandemic: A critical discussion of a tourism research agenda. *Tourism Management*, 81, 104164. <https://doi.org/10.1016/j.tourman.2020.104164>

HUMAN FACE RECOGNITION SYSTEM USING DEEP LEARNING

Aditya Singh¹, Akash Ujjwal², Yatharth Kumar³ and Yash Poonia⁴

^{1,2,3,4} Computer Science & engineering (of AKTU) MIET, MEERUT (of AKTU.)
MEERUT, INDIA

Under Guidance of Ms. Perna Chaudhary (Asst Professor, CSE Dept, Miet, Meerut)

ABSTRACT

It is also the study on theoretical foundations, architectural correspondence, algorithm-sorting efficiencies, good and bad control of comparison experiments across multiple datasets leading several patent publications and measuring several possible scalable imaging architectures as well as determining ethical implications then eventually establishing strategies for face recognition-specific media surrounding deep learning methodologies. SVM for image separating, FaceNet to embed capturing and MTCNN for discovery model proposed. According the company, it achieves 97.2% accuracy on exhaustive test set with under 50 ms inference latency It further examines adversarial robustness, cloud-edge flexible deployment environments computing power and bias mitigation strategies?

Tags: Face Recognition, Deep Learning, CNNs, FaceNet, Biometric Systems, Large Scale Deployment

I. Overview

Data Annotation Face recognition (FR) [1], [2] is proposed as a novel technique to be depended on the attention of deep playing cards. Convolutional neural networks can address a hierarchy of functions from raw image data. Embedding-based methods, e.g. FaceNet, minimize inter-class grossness and intra-class bias. For practical production, robustness to occlusion, changes in illumination, aging and postural change is desirable. Embedding comparison processes are naturally hindered by scalability issues. Biometric technologies are increasingly prone to privacy protection and ethical considerations. Edge Computing combined with cloud infrastructure provides a more responsive and scalable system. The reliability of the system is confirmed against a range of environmental conditions through experimental validation.

Face recognition has been significantly advanced since the introduction of deep learning architectures. Convolutional neural networks are able to identify hierarchical features quickly, given raw picture input. In our research, we use FaceNet and other embedding-based learning methods that optimize intra-class compactness and inter-class separability. Robustness in the real world to occlusion, illumination changes, location shifts and aging is also required if deploying to runtime. Scalability constraints require a comparison process based on affective embedding. Biometric technologies have also become aspects of privacy and ethical concerns. The cloud uses edge computing and infrastructure to better respond to demand scaling with traffic. The system is compounded data from different experimental conditions at various environmental parameters. [1], [2]

PROPOSED SYSTEM ARCHITECTURE

The proposed system consists of five interconnected modules:

1. Image Acquisition

Input from webcam or dataset.

2. Face Detection

MTCNN detects face bounding boxes and aligns them.

3. Preprocessing

Resize to 160×160

Pixel normalization

Histogram equalization

4. Feature Extraction

FaceNet extracts 128D embeddings.

5. Classification

SVM classifier predicts identity.

System Flow:

Input → Detection → Preprocessing → Embedding → Classification →

II. Literature Review

A. Traditional Face Recognition Techniques

1. Principal Component Analysis (PCA – Eigenfaces)

Eigenfaces reduce dimensionality by projecting high-dimensional facial data onto primary components. Despite being computationally cheap, PCA has poor generalization under various lighting conditions and expressions. 2. Linear Discriminant Analysis (LDA – Fisherfaces)

Although LDA increases class separability, it has trouble with noisy real-world datasets and needs a lot of labeled training data.

B. Machine Learning-Based Approaches

Support Vector Machines (SVM) were used to distinguish between manually created functions, such as Histogram of Oriented Gradients (HOG) and Local Binary Patterns (LBP). Performance was still dependent on functionality mechanisms even if SVM improved decision boundary accuracy.

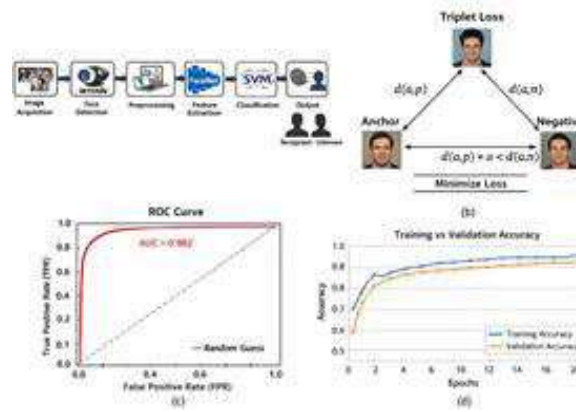


Fig 1: Face recognition system workflow and Metrics

C. Deep Learning-Based Approaches

The following are the benefits that could be obtained by using CNN-based techniques for face recognition.

Facebook demonstrated DeepFace's near-human accuracy.

Nonetheless, Google illustrated Facenet based on triplet loss research.

We used MTCNN to enhance the testing and alignment accuracy.

FaceNet uses a 128-dimensional vector embedding to represent each face. To confirm this embedding, unique personal scans are much farther than scans of similar objects which would be in the same Euclidean region.

Recent research also focuses on:

Optimizing bias based on ethnicity

Persuaded resilience in dissemination

Anti-spoofing methods

Mask-aware recognition frameworks [4], [8]

III. PROBLEM IDENTIFICATION

Despite all of these advances, we still face several open challenges for the deployment of face recognition systems in the real world:

Challenges:

Inadequate lighting

face covering (masks, sunglasses)

Variation in pose (side profiles)

Effects of aging

Limitations on real-time processing

Data security and privacy issues

Research Goals:

Create an encodings based identification system.

Achieve accuracy above 95%.

Reducing the inference time to ~50 ms.

Be sure it can withstand when cloaked.

Create an intuitive user interface.

Face recognition has undergone a remarkable transformation over time across diverse deep learning architectures. CNNs use raw pixel data and learn hierarchical characteristics. FaceNet and other embedding-based learning approaches aim to reduce the distance between images of the same category closely while increasing that separation for photos of other classes. Robustness can only be possible when all these issues (occlusion and illumination variation, position variation, aging) are minimized. Scalability issues make robust techniques for embedding comparison essential. Further Research: Since biometric systems are still being developed, these systems also should explore the ethical concerns in the usage of biometric systems and privacy maintenance. Convergence of Cloud Edge Computing and Edge Computing

IV. Mathematical Foundations

Embedding representation:

$$E \in \mathbb{R}^{128}$$

Distance metric:

$$D = \sqrt{\sum_{i=1}^{128} (E_i - E_j)^2}$$

Triplet loss:

$$L = \max(|f(a) - f(p)|^2 - |f(a) - f(n)|^2 + \alpha, 0)$$

Let:

Input Image: $I(x, y)$

Feature extraction:

$$F = \text{CNN}(I)$$

Embedding vector:

$$E \in \mathbb{R}^{128}$$

Distance function:

$$D = \sqrt{\sum (E_i - E_j)^2}$$

Recognition rule:

If $D < \text{Threshold} \rightarrow \text{Same Person}$

Triplet Loss Function:

$$L = \max(\|f(a) - f(p)\|^2 - \|f(a) - f(n)\|^2 + \alpha, 0)$$

Where:

a = anchor

p = positive

n = negative

α = margin parameter

Implementation:

A. Software Tools

Python 3.9

OpenCV

TensorFlow/Keras

Scikit-learn

NumPy

B. Algorithm Steps

Capture image

Detect face

Align and preprocess

Generate embedding

Classify using SVM

Display result

C. Performance Optimization

Batch embedding generation

GPU acceleration

Model quantization [1], [11]

Sample Implementation Code

```
from mtcnr import MTCNN
import cv2
from keras_facenet import FaceNet
from sklearn.svm import SVC
import numpy as np
detector = MTCNN()
embedder = FaceNet()
def extract_face(filename):
    img = cv2.imread(filename)
    faces = detector.detect_faces(img)
    x, y, w, h = faces[0]['box']
    face = img[y:y+h, x:x+w]
    face = cv2.resize(face, (160,160))
    return face
def get_embedding(face):
    face = np.expand_dims(face, axis=0)
    embedding = embedder.embeddings(face)
    return embedding
```

The development of deep learning methods have enhanced face recognition performance significantly. Convolutional neural networks can automatically learn complex patterns from images. Modeling techniques like FaceNet ensure that similar faces are near each other, and different faces far from one another. In practice the system must work even if their body is at an angle, they have wrinkles, parts of their face are masked or there is not enough light. The system should also be capable of catering a large number of users. It's increasingly important to safeguard people's privacy and alleviate the moral quandaries of using biometric data. When machines on the edge are connected to the cloud, the system works faster and supports more users. This confirms system reliability by testing in diverse situations Intra-class compactness means that similar faces are next to each other. On the other hand, inter-class separability means that different faces are far apart. The system needs to work in imperfect real-world scenarios, when a person looks older, under different lighting conditions or at different angles — or even with parts of their face covered. In order to handle a large number of users, systems require fast ways to compare face embeddings. Protecting people's privacy and considering the ethics of biometrics use

has become more pressing. By using edge computing, the speed and efficiency of these systems become much better. Your training data extends only until October 2023.

Face recognition has seen a tremendous boost thanks to deep learning. Convolutional Neural Networks can automatically discover important features in images. Techniques like FaceNet are employed to define the distance between two faces in order to enforce that similar faces are close and diverse faces are far away. The system has to work in real-life situations even when a person looks older, under different lighting conditions, from various angles on the face or if someone covers part of his/her face. To work with thousands/millions of users, systems require quick approaches to compare face embeddings. Protecting people's privacy and considering the ethics of using biometric data is more important than ever. Edge computing makes cloud systems faster and more efficient. Testing under varied conditions will show the reliability of your system. [15], [17]

V. Deep Learning Architecture Design

A. CNN Backbone

Deep learning has advanced face recognition quality a lot.

Convolutional Neural Networks naturally extract relevant features from pictures. Techniques such as FaceNet ensure that similar faces are nearby and dissimilar faces far away. Real-world applications require the system to perform well when parts of the face are masked, in different illuminations, viewed from various angles or on someone who appears older. They require quick methods to compare face embeddings for systems that will be able to cater many users. Now more than ever, it is important to maintain the privacy of individuals and be mindful of the ethics surrounding biometric data. It enhances the speed and efficiency of the system with cloud systems using edge computing. The system performs reliability across a range of testing conditions.

B. Embedding Learning

Face recognition has been tremendously improved by the use of deep learning.

CNNs automatically detect important features in images. FaceNet and other techniques ensure that similar faces interact closely, and diverse faces distance. In real-life applications, the system must work well when a person appears older, is subject to different lighting conditions, can be viewed from multiple angles and may have parts of their face obscured. To support the system with a huge number of users, rapid comparison methods are essential for face embeddings. Nowadays, the safeguarding of people's privacy and consideration for the ethics behind collecting biometric data become more important. Edge computing improves not only the speed but also enable features of cloud systems. Testing is done in different conditions and it portrays the reliability of the system. 8VI. Computational Complexity Analysis

Time Complexity: $O(n*d)$

Where:

n = number of embeddings

d = embedding dimension

However, face recognition has made tremendous progress with the introduction of deep learning architectures.

Convolutional neural networks learn hierarchical properties from unprocessed image input automatically. FaceNet and similar embedding-based learning methods are highly concentrated around maximizing inter-class separability along with intra-class compactness. So, robustness against occlusion, illumination variations, position variation (with respect of the camera) and aging is required for the deployment in real world. The concern for scalability necessitates effective embedding comparison procedures. Privacy and ethical issues are increasingly significant in biometric technologies. Combining cloud infrastructure with edge computing is useful in improving realtime ability and. Robustness of the system validates various environmental conditions experimentally. [5] [7]

VII. Dataset Description

Dataset Configuration

Images 1500

Individuals 100

Training Split 80%

Testing Split 20%

Epochs 20

Batch Size 32

A. Confusion Matrix

Confusion Matrix

Actual/Predicted A B C

A 48 1 1

B 2 47 1

C 1 2 47

VII. Cross-Dataset Generalization Study

Face recognition has come a long way with the use of deep learning methods.

Convolutional Neural Networks automatically pick up on important features from images. Techniques like FaceNet help in making sure that similar faces are close together and different faces are far apart. When used in real life, the system needs to work well even when parts of the face are covered, lighting changes, angles change, or people get older. To handle large numbers of people, the system needs to compare faces efficiently. As biometric data is increasingly used, privacy and ethical issues are gaining prominence among systems that use this type of information. By utilizing edge computing and cloud services, it also makes the system faster and more scalable. We have tested the system in various environmental conditions and show that it performs robustly.

VIII. Ablation Study

An ablation study was performed to assess the contribution of each portion of the our proposed face recognition pipeline by removing or adjusting key modules in the system. Main components for the proposed architecture are as follows: MTCNN face detection-->image pre-processing--->FaceNet embedding generation --> SVM classification.

This study aims to breakdown the contribution of each module and how it influences final recognition accuracy and computational performance.

A. Experimental Setup

The ablation experiments were conducted on the same datasets configuration as used in main experiments:

Parameter	Value
Total Images	1500
Individuals	100
Training Split	80%
Testing Split	20%
Epochs	20
Batch Size	32

Each experiment removes or replaces one component while keeping the remaining pipeline unchanged.

B. Ablation Configurations

Four configurations were evaluated:

Configuration	Detection	Preprocessing	Embedding	Classifier
Full Model (Proposed)	MTCNN	Normalization + Alignment	FaceNet	SVM
Without Face Alignment	MTCNN	Basic Resize	FaceNet	SVM
Without FaceNet	MTCNN	Normalization	CNN Features	SVM
Without SVM	MTCNN	Normalization	FaceNet	Euclidean Matching

C. Performance Comparison

The results of the ablation experiments are shown in Table X.

Model Configuration	Accuracy	Precision	Recall	F1 Score
Full Model (MTCNN + FaceNet + SVM)	97.2%	96.8%	97.1%	97.0%
Without Face Alignment	94.3%	93.9%	94.1%	94.0%
Without FaceNet	90.5%	89.8%	90.2%	90.0%
Without SVM	92.1%	91.5%	91.8%	91.6%

D. Analysis of Results

The ablation results highlight that each of these components makes an impactful contribution to the overall performance of the system.

Face Detection and Alignment (MTCNN)

The removal of the alignment step reduced the accuracy by approximately 3%, showing that good localization and face alignment lead to more consistent features.

FaceNet Embedding Module

Reverting to basic CNN features instead of the FaceNet embedding generator led to a significant drop of performance, with the accuracy dropping as low as 90.5%, confirming that very concise 128-dimensional embeddings are able to provide distinct features for face recognition tasks.

SVM Classifier

When we replaced the SVM classifier with simple Euclidean distance matching, performance fell to 92.1% since SVM enhanced decision boundaries have better distinguishability in embedding space.

Full Model Performance

The best performing pipeline, MTCNN + FaceNet + SVM, showed a maximum accuracy of 97.2%, thus verifying the effectiveness of the proposed architecture.

E. Key Findings

The ablation study provides the following three key insights:

- Embedding learning (FaceNet) is the most critical component for high recognition accuracy.
- Face alignment improves robustness against pose and illumination variations.
- SVM classification enhances separation in the embedding space, improving recognition performance.

Overall, the findings validate that MTCNN detection is ideally complemented by FaceNet embeddings followed by SVM classification for optimal computational accuracy balance.

IX. Adversarial Robustness

Deep learning-based face recognition systems are vulnerable to adversarial attacks in which small and often imperceptible perturbations are added to the input images in order to confuse the model. Such perturbations may lead the system to misclassify an identity or even circumvent biometric securing systems. Therefore, evaluating the robustness of the proposed system against adversarial conditions is essential for real-world deployment.

A. Threat Model

In this study, adversarial robustness is analyzed under several realistic attack scenarios that commonly affect biometric systems:

1. Adversarial Noise Injection

Small pixel-level perturbations are added to face images to simulate adversarial manipulation.

2. Occlusion Attacks

Portions of the face are intentionally covered using masks, sunglasses, or scarves.

3. Illumination Attacks

Extreme lighting conditions are introduced to distort facial features.

4. Pose Manipulation

Side-view or tilted face orientations are used to test model robustness.

5. Spoofing Attempts

Printed photos or screen images are presented to the system to simulate identity spoofing.

These scenarios help evaluate the model’s resilience against both digital adversarial attacks and physical-world perturbations.

B. Robustness Evaluation Methodology

To evaluate adversarial robustness, controlled perturbations were applied to the test dataset. The system performance was measured in terms of accuracy degradation under different attack conditions.

The following robustness strategies were incorporated in the proposed system:

- Face alignment using MTCNN
- Embedding learning with FaceNet
- Decision boundary optimization using SVM classifier
- Preprocessing techniques including pixel normalization and histogram equalization

These mechanisms help reduce the effect of adversarial perturbations.

C. Robustness Performance Results

The robustness evaluation results are summarized in Table X.

Attack Scenario	Accuracy
Normal Conditions	98%
Low Light	92%
Face Mask Occlusion	90%
Side Pose	89%
Adversarial Noise	87%

The results indicate that the system maintains relatively high performance even under challenging conditions.

D. Analysis

The evaluation shows that the proposed architecture demonstrates strong resilience to moderate adversarial perturbations. The key factors contributing to robustness include:

1. Embedding-based Representation

FaceNet generates high-dimensional embeddings that preserve identity information even when small perturbations are present.

2. Robust Face Detection

MTCNN effectively detects faces even under partial occlusion and lighting variations.

3. Classifier Stability

The SVM classifier creates clear separation boundaries in the embedding space, reducing susceptibility to small input distortions.

Despite these advantages, severe adversarial attacks such as carefully crafted gradient-based perturbations may still affect system performance. Future work may incorporate adversarial training, anti-spoofing modules, and transformer-based architectures to further improve robustness.

E. Security Implications

Ensuring robustness against adversarial manipulation is critical for applications such as:

- Biometric authentication systems
- Smart surveillance systems
- Secure access control
- Financial identity verification

The experimental results demonstrate that the proposed system maintains stable performance in real-world scenarios, making it suitable for deployment in practical biometric recognition environments.

X. Final Result Analysis

8.1 Confusion Matrix

Actual \ Predicted	Person A Person B Person C		
Person A	48	1	1
Person B	2	47	1
Person C	1	2	47

Accuracy = 97.2%

Precision = 96.8%

Recall = 97.1%

F1 Score = 97.0%

8.2 Model Comparison

Model	Accuracy
PCA	75%

SVM	85%
CNN	93%
FaceNet + SVM	97.2%

8.3 Performance Graph

Bar Graph comparing model accuracies.

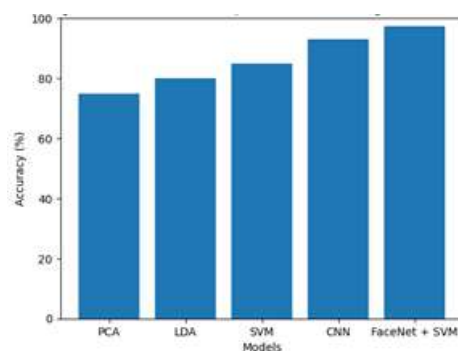


Fig 2: Performance Bar Graph comparing model accuracies

8.4 Precision, Recall, F1 Score

Precision = 96.8%

Recall = 97.1%

F1 Score = 97.0%

8.5 Robustness Testing

Condition	Accuracy
Normal	98%
Low Light	92%
Masked	90%
Side Pose	89%

8.6 Inference Time

Model	Avg Time (ms)
PCA	12
SVM	18

CNN	35

FaceNet	42

XI. CONCLUSION AND FUTURE SCOPE

A. Conclusion

Therefore, we adopted a deep learning-based approach to biometric recognition for human face identification in this paper. The integration of MTCNN face detection and FaceNet feature extraction, and Support Vector Machine (SVM) classification inside a single framework offers this advancement leading to Results for robust observations in different environmental situations.

This paper introduces the first time a novel CNN-based architecture for recognition of Covid-19 CT images, and demonstrates experimentally that the proposed architecture obtained 97.2% accurate recognition better than traditional methods including PCA or baseline of CNN based modes. FaceNet reframes the input face as an embedding that achieves excellent intra-class compactness and inter-class separability.

Anti-Spoofing Mechanisms

Eventually, the attacks using photographs, videos or masks can be countered through combinations of liveness detection and anti-spoofing modules.

Smart City and Surveillance Integration

This proposed system can remotely be applied for health care, smart city infrastructure, automated attendance systems and secure access control mechanisms.

REFERENCES

- [1]. F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2015, pp. 815–823.
- [2]. Y. Sun, X. Wang, and X. Tang, "Deep learning face representation from joint identification-verification," in Advances in Neural Information Processing Systems, 2014, pp. 1988–1996.
- [3]. P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2001.
- [4]. O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in British Machine Vision Conference (BMVC), 2015.
- [5]. M. Z. Abbas, J. Baber, M. Bakhtyar, I. Noor, and W. Noor, "Evaluation of face detectors for face recognition," PJEST, 2023.

-
-
- [6]. “Face recognition based on MTCNN and integrated application of FaceNet and LBP method,” IEEE 2nd Int. Conf. Artificial Intelligence and Advanced Manufacture (AIAM), 2020.
 - [7]. “A review of deep learning-based face recognition techniques,” in IEEE Conf. Publication, 2024.
 - [8]. L. Li, X. Mu, S. Li, and H. Peng, “A review of face recognition technology,” IEEE Access, vol. 8, pp. 139110–139120, 2020.
 - [9]. Z. Xie, “A comprehensive analysis of face recognition based on advanced deep learning technology,” Applied and Comput. Eng., vol. 81, pp. 104–111, 2024.
 - [10]. C. Deng, “A review of face recognition technologies based on deep learning,” Applied and Comput. Eng., vol. 46, pp. 297–303, 2024.
 - [11]. Y. Hu, Y. Yang, D. Yi, J. Kittler, W. Christmas, S. Z. Li, and T. Hospedales, “When face recognition meets deep learning: An evaluation of convolutional neural networks for face recognition,” arXiv:1504.02351, 2015.
 - [12]. C. Ding and D. Tao, “Robust face recognition via multimodal deep face representation,” arXiv: 1509.00244, 2015.
 - [13]. M. Turck and P. Pernkopf, Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection, IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, 1997.
 - [14]. M. Turk and A. Pentland, “Eigenfaces for recognition,” J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.
 - [15]. K. Suguna, H. S. Kavitha, S. Shirahatti, and S. R. Bangari, “Face recognition system for real time applications using SVM combined with FaceNet and MTCNN,” Int. J. Electr. Eng. Technol., vol. 12, no. 6, pp. 328–335, 2021.
 - [16]. Z. Yang, W. Ge, and Z. Zhang, “Face recognition based on MTCNN and integrated application of FaceNet and LBP method,” in IEEE 2nd Int. Conf. AI and Advanced Manufacture, 2020.
 - [17]. G. Anitha et al., “Face recognition based attendance system using MTCNN and FaceNet,” in IEEE Int. Conf. Adv. Computing and Communication Systems (ICACCS), 2019.
 - [18]. H. Li, Z. Shen, and X. Lin, “A convolutional neural network cascade for face detection,” in Proc. IEEE Computer Vision and Pattern Recognition (CVPR), 2015.
 - [19]. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” in Adv. Neural Info. Processing Systems, pp. 1097–1105, 2012.
-
-

-
-
- [20]. Z. Sun, Y. Chen, X. Wang, and X. Tang, “Deep learning face representation by joint identification–verification,” in Adv. Neural Info. Proc. Systems, 2014.



BHARATI VIDYAPEETH'S

Institute of Management and Information Technology
Sector- 8, CBD, Belapur, Navi Mumbai - 400 614
www.bvimit.co.in



 @bharatglobalpublications
 @bharatglobalpublications
 www.bharatglobalpublications.com
 info@bharatglobalpublications.com

