



AI-Driven Voter Authentication and Fraud Detection System

Dr V Seedha Devi¹, Kaavya S², Deepika B³, Jayashree D⁴, Nithikaa L⁵

Associate Professor, Department of Information Technology, Jaya Engineering College, Anna University, Chennai,
Tamil Nadu, India¹

UG Student, Department of Information Technology, Jaya Engineering College, Anna University, Chennai,
Tamil Nadu, India^{2,3,4,5}

Publication History: Received: 02.04.2026; Revised: 03.05.2026; Accepted: 05.05.2026; Published: 09.05.2026.

ABSTRACT: Ensuring election integrity is crucial to uphold democratic values and prevent fraudulent activities such as fake voting and multiple voting attempts. Traditional voter verification methods, such as checking physical identity cards or signatures, can be easily manipulated or forged, leading to potential electoral fraud. Biometric systems, especially fingerprint recognition, are widely acknowledged as reliable because fingerprints are unique to each individual and difficult to replicate or fake. Fingerprint authentication eliminates the need for voters to carry physical IDs or documents, which can be lost, forged, or misused, making the voting process more secure and efficient. In the proposed system, fingerprint scanning serves as the first line of defense against fake voters. At the polling station, every voter is required to place their finger on a fingerprint scanner. The system compares the scanned fingerprint with a pre-registered fingerprint database that contains data of all eligible voters. If the scanned fingerprint matches a registered voter's fingerprint, the system confirms the voter's identity and eligibility to vote. Therefore, to add a second layer of security, an OTP (One-Time Password) verification step is integrated into the system. Once the fingerprint scan is successful, an OTP is automatically generated and sent to the voter's registered mobile number. The voter must enter this OTP at the polling terminal to confirm that they are in physical possession of their phone linked with the registered voter profile. This OTP verification acts as a dynamic security token, making it extremely difficult for someone to vote using stolen or fake biometric data.

KEYWORDS: OTP Verification, Iris Scanner, Fingerprint Sensor, Neon Database, 2 Step Verification., Artificial Intelligence.

I. INTRODUCTION

Artificial Intelligence (AI) is one of the most rapidly growing fields of computer science that focuses on creating machines and software capable of performing tasks that normally require human intelligence. These tasks include learning from experience, understanding natural language, recognizing patterns, solving problems, making decisions, and even showing creativity. In simple terms, Artificial Intelligence is the ability of a machine to think, learn, and act like a human. The concept of Artificial Intelligence is not new. The idea of intelligent machines dates back to ancient myths and philosophical discussions, but AI as a scientific field began in the mid-20th century. In 1956, the term "Artificial Intelligence" was officially introduced by John McCarthy at the Dartmouth Conference. Since then, AI has evolved from simple rule-based systems to advanced technologies such as machine learning, deep learning, and neural networks. Today, Artificial Intelligence plays a vital role in our daily lives, often without us even realizing it. From voice assistants like Siri, Alexa, and Google Assistant to recommendation systems on Netflix, YouTube, and Amazon, AI is everywhere.

II. LITERATURE REVIEW

Goma E1, Manasa G2, Manjula B3, and Sanchana S4 Proposes a multi-factor biometric voting system using deep learning techniques. It uses Convolutional Neural Networks (CNNs) to process iris, face, and fingerprint data for voter authentication. The system achieves high accuracy by combining multiple biometric layers and OTP verification, reducing impersonation and fraud. The integration of CNN improves feature extraction and matching performance.



However, the system requires high computational power (GPU support) and raises privacy concerns due to storage of multiple biometric data.

T. Keerthi, M. C Chinnaiah, Apurva Kumari, Asharani P., D. Harikrishna, and G. Divyavani presents a fingerprint-based voting system integrated with IoT technology. It uses basic fingerprint authentication controlled by an Arduino Uno and data transmission through an ESP8266 module. The system ensures accurate voter verification and real-time result monitoring using cloud platforms. It improves transparency and reduces manual errors in voting. However, it mainly relies on single-factor authentication and has limited scalability, making it less suitable for large-scale elections. R. Karthik, S. Karthikeyan, P. Harish, and M. Dinesh proposed a secure electronic voting system using biometric fingerprint authentication for voter verification. This paper introduces an iris recognition-based e-voting system using deep learning. It uses a ResNet-18 model for feature extraction and cosine similarity for matching iris patterns. The system achieves high accuracy (~99.2%) even under varying environmental conditions. It provides secure and fast authentication through biometric templates stored in a database. However, the system requires specialized hardware (iris scanner) and high computational resources, which may increase cost.

S. Kavitha, R. Sangeetha, P. Deepa, and M. Nandhini proposed an electronic voting system using biometric authentication to ensure secure voter identification. This study proposes a facial recognition voting system using enhanced ResNet50 architecture along with MTCNN for face detection and Arc Face loss function. It achieves a high accuracy of around 99.56% in voter authentication. The system effectively prevents multiple voting and improves reliability using deep learning techniques. However, its performance depends on lighting conditions and camera quality, and it may face privacy issues due to facial data storage.

A. Ramesh, B. Suresh, C. Priya, and D. Karthika proposed a smart electronic voting system using biometric authentication to ensure secure and accurate voter identification. This paper presents a digital voting system using face recognition techniques for voter authentication. It uses standard face recognition algorithms with a web-based system to ensure fast verification and automatic vote counting. The system improves efficiency by reducing voting time and providing instant results. It ensures “one person, one vote” with good accuracy in controlled environments. However, it has scalability limitations and lacks advanced liveness detection, making it less secure against spoofing attacks.

III. PROBLEM STATEMENT

The existing process of voter fraud detection relies on a combination of administrative checks, biometric authentication, technological controls, and legal enforcement applied before, during, and after elections. Initially, voter registration databases are verified to eliminate duplicate, deceased, or ineligible voters. Electoral roles are periodically audited and cross-validated with government records to identify anomalies. At polling stations, voter identity is verified using official voter ID documents, and in some systems, biometric verification methods such as fingerprint or facial recognition are employed to prevent impersonation. In several countries, indelible ink is applied to voters' fingers to restrict repeat voting. Polling officials and election observers monitor voter behavior to detect suspicious activities, while surveillance cameras are used to discourage organized fraud. Electronic voting systems may incorporate real-time validation mechanisms to block multiple votes from the same voter. After voting, turnout data is cross-checked with vote counts to detect inconsistencies. Statistical and forensic analysis of ballots or electronic logs is conducted to identify irregular voting patterns. Election monitoring bodies investigate reported fraud cases, supported by legal frameworks that define penalties for electoral offenses. Cybersecurity monitoring is also used to detect hacking attempts or manipulation of digital voting systems.



IV. RESEARCH METHEDOLOGY

4.1 System Architecture

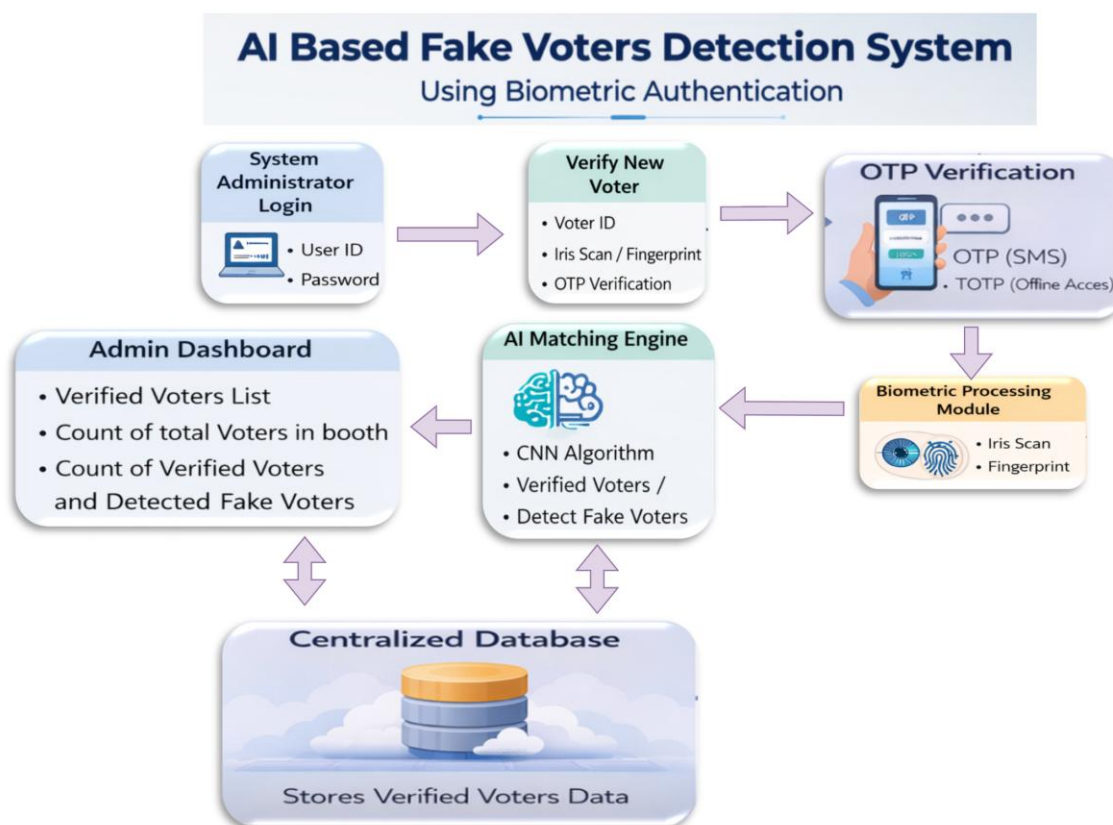


Fig.1. Architecture of an AI-Based Fake Voter Detection

User Registration Module

It is one of the most important components of the AI Based Fake Voters Detection System. This module is primarily handled by the administrator and is responsible for enrolling eligible voters into the system before the election process begins. During registration, essential details such as the voter's full name, voter ID number, date of birth, address, and registered mobile number are collected and verified. In addition to basic information, biometric data including fingerprint and iris scans are captured using biometric devices. These biometric details serve as a unique identity for each voter and help prevent duplicate registrations and impersonation.

Authentication Module

It is a critical component of the AI Based Fake Voters Detection System, designed to ensure that only legitimate and eligible voters are allowed to cast their votes. This module implements a multi-level verification process to enhance security and prevent unauthorized access. The authentication process begins when the voter enters their Voter ID and registered mobile number into the system. The system verifies these details with the stored records in the database to confirm the voter's identity and eligibility status.

AI Matching Module

This Module is one of the most critical components of the AI Based Fake Voters Detection System. Its primary purpose is to identify and prevent fake voters, duplicate registrations, and impersonation attempts during the voting process. The AI module processes this data using advanced feature extraction and pattern recognition algorithms. Unique biometric features such as ridge patterns in fingerprints and texture patterns in iris images are converted into digital templates. This module uses Artificial Intelligence and machine learning algorithms to analyze biometric data and detect suspicious patterns in real time.



Admin Dashboard Module

The Admin Dashboard module plays a crucial role in the AI-based Fake Voters Detection System using Biometric Authentication and OTP Verification. It acts as the central control interface that allows the election administrator to monitor and manage the voter verification process in real time. Through the dashboard, the admin can view important information related to the voting booth, such as the total number of registered voters, the number of voters who have been successfully verified, and the number of fake or suspicious voters detected by the system.

Testing Methodology: The system testing process follows a structured methodology:

1. **Unit Testing:** Individual components (e.g., sensors, microcontroller, mobile app) are tested for functionality and accuracy.
2. **Integration Testing:** The system components are integrated, and testing is performed to ensure they work together as expected.
3. **System Testing:** The complete system, including hardware, software, and connectivity, is tested for overall performance, reliability, and usability.
4. **Acceptance Testing:** The system is tested in real-world scenarios, ensuring that it meets the needs and requirements of users and healthcare professionals.
5. **Regression Testing:** Any changes or updates to the system are re-tested to ensure they do not affect existing functionality.

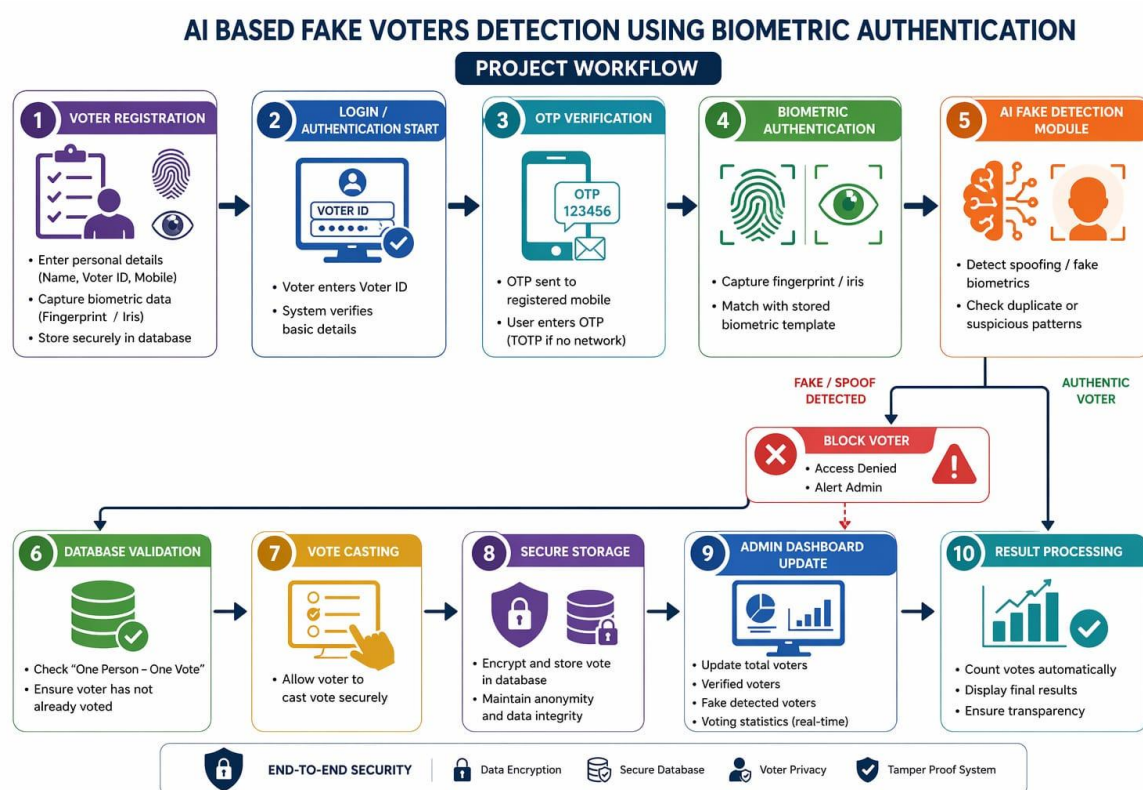


Fig.2. Research Workflow

V. RESULT

The system should accurately authenticate voters using multi-factor verification. AI-based detection should successfully identify duplicate or fake voter attempts. Each voter should be allowed to vote only once. Votes should be securely encrypted and stored without revealing voter identity. The system should operate smoothly with minimal response time. The admin panel should accurately monitor and report suspicious activities.



Output

The image shows the 'SECUREVOTE' login interface. At the top, the title 'SECUREVOTE' is in large, bold, white letters, with the subtitle 'Access Your Account' below it. There are two buttons: 'Voter Login' (highlighted in red) and 'Admin Login' (in grey). Below these are two input fields: the first is labeled with a calendar icon and contains the text 'VOTER1776184542756649'; the second is labeled with a person icon and contains the email 'kaavya1905@gmail.com'. At the bottom is a large red 'Login' button.

Fig.3. Voter Login Page

This Fig.3 shows the login interface of the SecureVote system, designed for secure online voting access. It provides separate login options for voters and administrators, along with fields for voter ID and registered email address. The login page ensures authorized and secure access to the voting platform before entering the sys

The image shows the 'Verify Your OTP' page. At the top, there is a small blue circle containing a 2x2 grid of numbers (1, 2, 3, 4). Below this, the title 'Verify Your OTP' is in large, bold, white letters, followed by the subtitle 'Enter the code sent to kaavya1905@gmail.com'. There is a red button that says 'Check your email for the 6-digit code'. Below this are six empty square boxes for entering the OTP digits. At the bottom is a large red 'Verify OTP' button, and a '← Back' link is visible below it.

Fig.4. OTP Verification Page

This Fig.4 shows the OTP verification page of the SecureVote system used for second-factor authentication. It prompts the user to enter the 6-digit code sent to their registered email address to confirm their identity. This step adds an extra layer of security and prevents unauthorized access to the voting system.

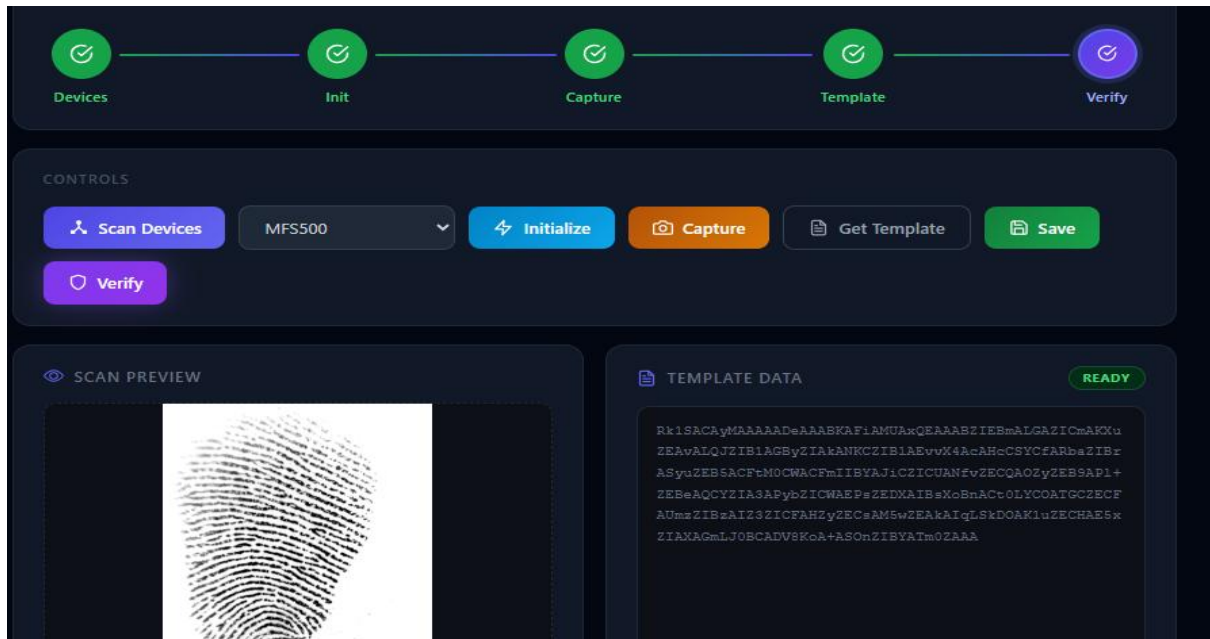


Fig.5. Fingerprint Verification Page

The Fig.5 shows the fingerprint verification interface used for biometric authentication in the secure Vote system. It guides the user through steps such as device selection, initialization, fingerprint capture, template generation, and verification.

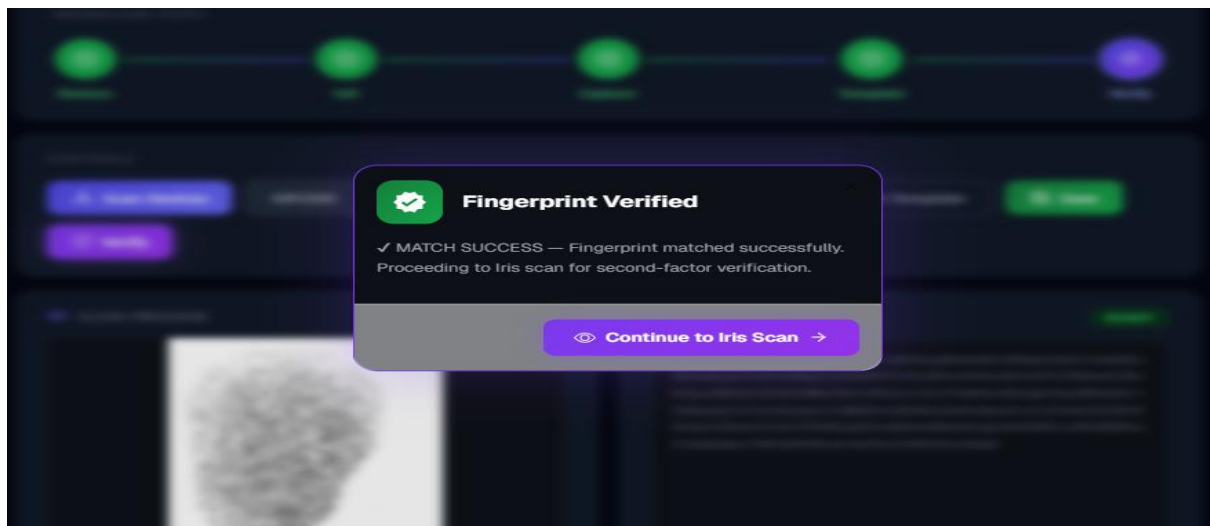


Fig.6. Fingerprint Verification Successful Page

The Fig.6 shows the successful fingerprint verification confirmation in the secure Vote system. It indicates that the captured fingerprint has matched successfully with the stored biometric data of the voter. After verification, the system allows the user to proceed to the next security step, which is iris scanning.

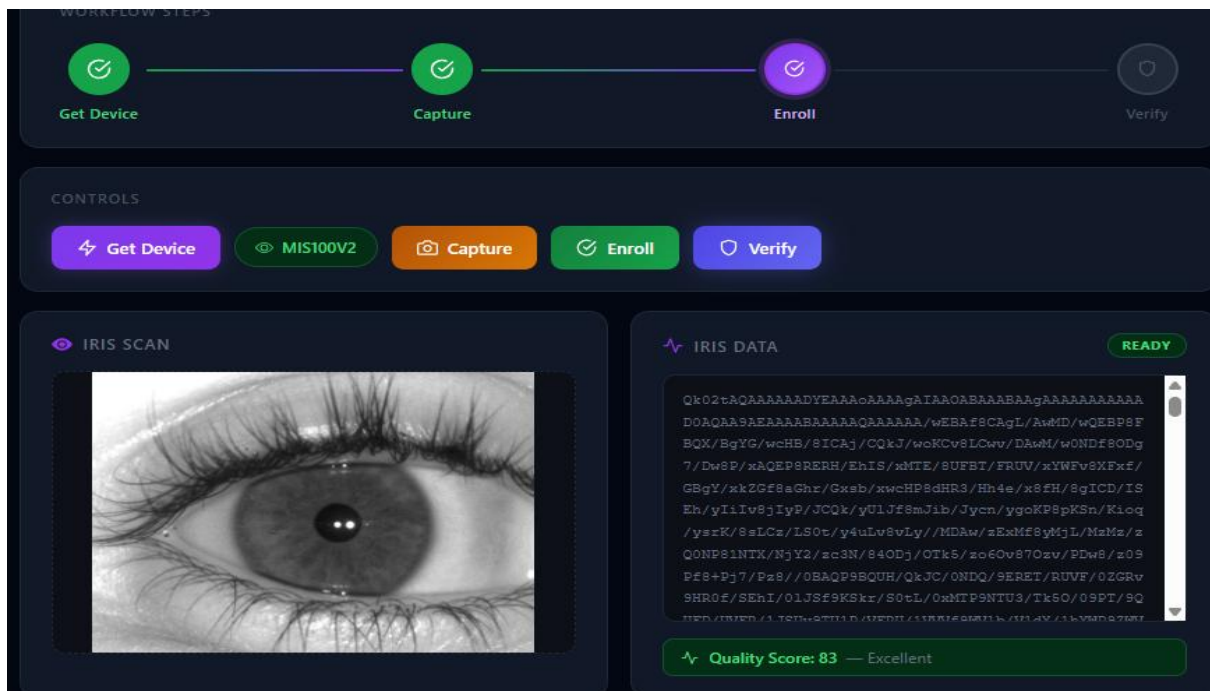


Fig.7. Iris Capture Page

The Fig.7 shows the iris verification module used as an advanced biometric authentication step in the Secure Vote system. It captures the voter's iris image and converts it into encrypted iris data for identity verification. This process provides high-level security by ensuring accurate voter authentication before voting access.

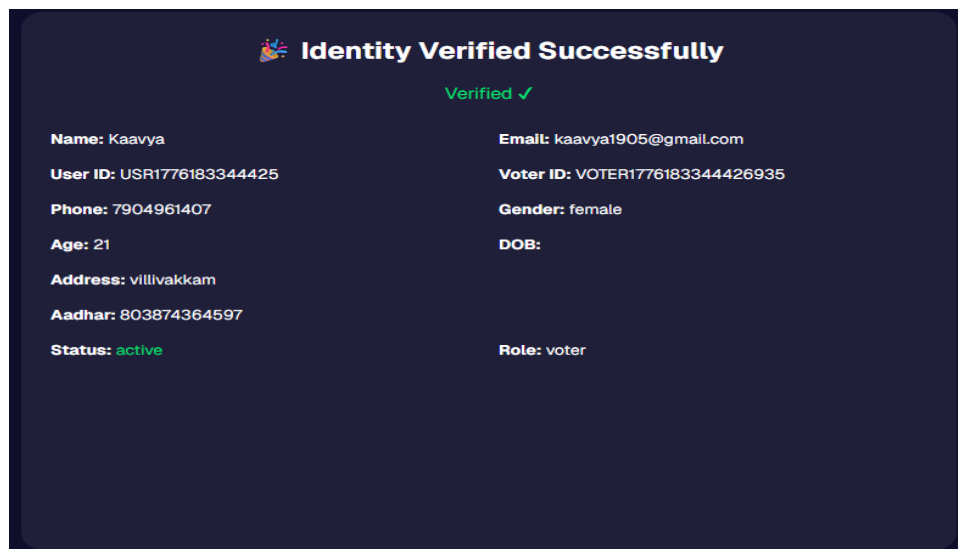


Fig.8. Verification Successful Page

The Fig.8 shows a successful identity verification screen for a voter in an electronic voting system. It displays personal details like name, user ID, voter ID, contact information, and Aadhaar number. The status is marked as “Verified,” indicating the user is authenticated and eligible to vote.

**VI. CONCLUSION AND FUTURE ENHANCEMENT**

The AI Based Fake Voters Detection System using Biometric Authentication presents an innovative and secure approach to modern electronic voting. This system successfully demonstrates how advanced technologies such as Artificial Intelligence, biometric authentication (fingerprint and iris recognition), OTP verification, and secure database management can be integrated to create a transparent and tamper-proof voting platform. The project addresses major challenges faced in traditional voting systems, including duplicate voting, identity impersonation, and electoral fraud. By implementing multi-factor authentication and AI-based fake detection mechanisms, the system ensures that only genuine and eligible voters can cast their votes. The encryption of voting data and separation of voter identity from vote records guarantee confidentiality and anonymity, which are fundamental principles of democratic elections. The integration of frontend technologies (React), backend frameworks (Node.js and Express.js), database management (MongoDB), and AI-based biometric comparison have proven the feasibility of building a scalable and secure voting infrastructure. The system also provides administrative monitoring capabilities, enabling real-time supervision and detection of suspicious activities. Overall, the project demonstrates that combining biometric verification with intelligent fraud detection significantly enhances election integrity, security, and trustworthiness. The developed system serves as a strong foundation for implementing secure digital voting solutions in future electoral processes.

The AI Based Fake Voters Detection System provides a secure and efficient voting mechanism, several enhancements can further improve its functionality and scalability. One important enhancement is the integration of advanced machine learning models capable of continuously learning from new fraud patterns. This would improve detection accuracy and reduce false positives over time. The implementation of blockchain technology could also be considered to create an immutable and transparent ledger for vote storage, further strengthening trust and tamper resistance. Another future enhancement involves expanding biometric capabilities to include facial recognition with liveness detection, ensuring stronger identity verification while preventing spoofing attacks. Cloud-based deployment with distributed server architecture can improve scalability, allowing the system to handle large-scale national elections with millions of voters simultaneously. Improving accessibility features such as multilingual support, voice-guided assistance, and simplified user interfaces would make the system more inclusive for elderly and differently abled voters. Additionally, integrating real-time analytics dashboards for election authorities can provide insights into voter turnout, system health, and anomaly detection. Enhancing cybersecurity measures through advanced encryption standards, intrusion detection systems, and regular vulnerability assessments will further strengthen system resilience against cyber threats. These future enhancements will transform the AI Based Fake Voters Detection System into a highly secure, scalable, and intelligent digital voting platform capable of supporting modern democratic processes with greater efficiency and reliability.

REFERENCES

- 1) Goma E., Manasa G., Manjula B., Sanchana S., "Iris Recognition Based Modern Voting System Using Deep Learning", International Journal for Multidisciplinary Research (IJFMR), E-ISSN: 2582-2160, Volume 7, 2025.
- 2) Zakiah Mohd Yusoff, Yusradini Yusnoor, Arni Munira Markom, Siti Aminah Nordin, Nurlaila Ismail, "Fingerprint Biometric Voting Machine Using Internet of Things", Indonesian Journal of Electrical Engineering and Computer Science, ISSN:2502-4752, Volume 30, 2023.
- 3) T. B. Karthikeyan, M. G. I. Jithamanyubabu, S. Subashini "E-Voting with Iris Recognition Using ResNet", International Journal for Research in Applied Science & Engineering Technology (IJRASET), ISSN:2502-4752, Volume 13, 2025.
- 4) Aminou Halidou, Daniel Georges Olle Olle, Arnaud Nguembang Fadja, Daramy Vandi Von Kallon, Tchana Ngninkeu Gil Thibault, "Voter Authentication Using Enhanced ResNet50 for Facial Recognition", Signals, MDPI, ISSN: 2624-6120, Volume 6, 2025.
- 5) Hayath T. M., Rajeev D. V., R. Nihanth, U. Venkata Tharun, R. Achutha "Digital Voting System with Face Recognition", International Journal of Scientific Research and Technology, ISSN: 2394-7063 Volume 3, 2026.
- 6) S. R. Prakash, L. V. N. Prasad, K. Mounika, P. Harshitha, M. Tejaswini, "AI-Based Secure Electronic Voting System Using Multi-Biometric Authentication", Procedia Computer Science, ISSN:1877-0509, Volume 235, 2024.
- 7) R. K. Sharma, V. Priyanka, A. K. Singh, S. R. Devi, "Blockchain Integrated Biometric Voting System for Transparent Elections", International Journal of Information Technology, ISSN: 2511-2104, Volume 16, 2024.
- 8) M. A. Rahman, T. Hossain, N. Sultana, M. R. Islam, "Deep Learning-Based Fake Identity Detection in E-Governance Applications", Computers & Security, ISSN: 0167-4048, Volume 134, 2024.
- 9) [9] P. Anusha, K. R. Reddy, B. V. Kumar, "Fingerprint and Iris Fusion Model for Secure E-Voting System", Indonesian Journal of Electrical Engineering and Computer Science, ISSN: 2502-4752, Volume 32, 2024.



- 10) J. H. Lee, S. Y. Kim, D. W. Park, "Lightweight CNN Model for Real-Time Biometric Verification in National Voting Systems", IEEE Access, ISSN: 2169-3536, Volume 12, 2024.
- 11) K. Verma, S. Tiwari, R. Bansal, "Secure OTP and Biometric-Based Digital Voting Architecture", International Journal of Scientific Research in Computer Science Engineering and Information Technology, ISSN: 2456-3307, Volume 9, 2024.
- 12) N. El-Gohary, M. Hassan, A. A. Abdelrahman, "Anomaly Detection in Electronic Voting Systems Using Artificial Intelligence", Journal of Cybersecurity and Privacy, ISSN: 2624-800X Volume 4, 2024.
- 13) Seedha Devi, V., Harshini, R., Dhana Lakshmi, E., Gayathri, N., & Nithesha, P. (2026). Low-code mobile application builder with AI-assisted features using Flutter & Firebase. International Journal of Research Publications in Engineering, Technology and Management (IRPETM), 9(3), 1001–1010. <https://doi.org/10.15662/IRPETM.2026.0903001>
- 14) Vimal, V. R., & Banerjee, J. S. (2025). Integrating PSO, GA, and ACO for Optimized ECG Feature Selection and Classification of Cardiac Disorders. SGS-Engineering & Sciences, 1(5).
- 15) Aashiq Banu, S., Rao, L. K., Priya, P. S., Thanikaiselvan, Hemalatha, M., Dhivya, R., & Rengarajan, A. (2025). A review of genome to chaos: exploring DNA dynamics in security. Multimedia Tools and Applications, 84(22), 24859-24886.
- 16) Seedha Devi, V., Divya Narasimman, S., Jayaprakash, S., & Mohamed Suhel, H. N. (2026). Smart IoT-based pedestrian power generator using DC motor. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(3), 990–999. <https://doi.org/10.15680/IJCTECE.2026.0903002>
- 17) Anand, L., Tyagi, R., & Mehta, V. (2024, January). Food recognition using deep learning for recipe and restaurant recommendation. In Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 269-279). Singapore: Springer Nature Singapore.
- 18) Rajasekar, M., Arunachalam, P., Priyadharsini, P., Devi, N. L., Abbas, H. H., & Al-Qaisy, S. A. (2024, May). An optimized framework development of ABC algorithm along with SVM algorithm for lung cancer detection. In 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) (pp. 184-187). IEEE.
- 19) Mathew, A. (2025). Human-AI Collaboration in Security Operations: Measuring Alert Trust, Automation Bias, and Analyst Upskilling in AI-Augmented SOC Environments. International Journal of Computer Technology and Electronics Communication, 8(5), 11375-11380.
- 20) Sugumar, R. (2025). Federated AI in Offline-First Mobile Health Architectures for Privacy-Preserving Clinical Intelligence. International Journal of Science, Research and Technology, 8(4), 14589-14600.
- 21) Deivendran, P., Babu, P. S., Malathi, G., Anbazhagan, K., & Kumar, R. S. (2023). Emotion Recognition for Challenged People Facial Appearance in Social using Neural Network. arXiv preprint arXiv:2305.06842.
- 22) Seedha Devi, V., Mahalakshimi, P. V., & Anitha, A. (2026). Automated skin disease analysis and detection using AI-powered mobile application. International Journal of Research and Applied Innovations (IJRAI), 9(3), 531–539. <https://doi.org/10.15662/IJRAI.2026.0903004>
- 23) Rachana, P., Kalyan, P. P., Kumar, T. S., Reddy, P. M., Rohan, P., Saravanan, M., & Dharnasi, P. (2026). Secure Chat Application with End-To-End Encryption by using Deep Learning. International Journal of Computer Technology and Electronics Communication, 9(2), 472-478.
- 24) Alangaram, S., Udaykiran, M., Rajkumar, K., & Yogeewaran, T. (2026). Enhancing customer churn prediction and retention for e-commerce. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 803–813. <https://doi.org/10.15662/IJARCST.2026.0903003>
- 25) Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
- 26) Alangaram, S., Kiswar, M., Ajay, B., & Ezhilkumaran, P. (2026). Socialflow AI: Voice to social media scheduler. International Journal of Research and Applied Innovations (IJRAI), 9(3), 540–547. <https://doi.org/10.15662/IJRAI.2026.0903005>
- 27) Revathi, K. G., Ananth, B. J., Saravanan, M. L., & Kumar, A. R. (2021). Gps enabled vehicle location identification using gsm and fare collection using smart card. Turkish journal of computer and mathematics education, 12(10), 2657-2668.
- 28) Raghul, K., Rajasolan, P., Rohinth, S., & Tharun, P. (2026). AI knowledge sharing web portal. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 9(3), 814–823. <https://doi.org/10.15662/IJARCST.2026.0903004>
- 29) Mathew, A. A Secure, Trustworthy, and Regulated Framework for AI Agents in Distributed Networks.
- 30) Sangeetha, D., Dharan, K. D., Krishna, A. C., & Karthikeyan, C. (2026). Speech and text conversion system for sign language using ML. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(3), 1000–1007. <https://doi.org/10.15680/IJCTECE.2026.0903003>



- 31) Sulthana, A. R., & Murugeswari, B. (2011, March). ARIPSO: Association rule interactive postmining using schemas and ontologies. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 941-946). IEEE.
- 32) Rajasekar, M. (2025). Risk-Aware Generative AI and Machine Learning Frameworks for Privacy-Preserving Banking and Trade Analytics over Cloud and 5G Networks. *International Journal of Computer Technology and Electronics Communication*, 8(4), 11078-11086.
- 33) Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. *International Journal of Advanced Engineering Science and Information Technology (IAESIT)*, 8(5), 17261.
- 34) Sharma, K. P., Kumar, I., Singh, P. P., Anbazhagan, K., Albarakati, H. M., Bhatt, M. W., ... & Rana, A. (2024). Advancing spacecraft rendezvous and docking through safety reinforcement learning and ubiquitous learning principles. *Computers in Human Behavior*, 153, 108110.
- 35) Anand, L., & Syed Ibrahim, S. P. (2018). HANN: a hybrid model for liver syndrome classification by feature assortment optimization. *Journal of medical systems*, 42(11), 211.
- 36) Raj, T. S., Thangam, S. A., Balakrishnan, T. S., Ponnaian, G., & Vimal, V. R. (2025, July). Improving Object Detection in Low Light Surveillance Using Hybrid Image Fusion Techniques Over Traditional Filtering Methods. In 2025 2nd International Conference on Computing and Data Science (ICCDs) (pp. 1-6). IEEE.
- 37) Padmapriya, V. M., Thenmozhi, K., Hemalatha, M., Thanikaiselvan, V., Lakshmi, C., Chidambaram, N., & Rengarajan, A. (2025). Secured IIoT against trust deficit-A flexi cryptic approach. *Multimedia Tools and Applications*, 84(9), 5625-5652.
- 38) Seedha Devi, V., Harshini, R., Dhana Lakshmi, E., Gayathri, N., & Nithesha, P. (2026). Low-code mobile application builder with AI-assisted features using Flutter & Firebase. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 9(3), 1001–1010.