Fraud-Resistant Voting Using Aadhaar Authentication

Prof. Shwetha R[1], Priya G[2], Gowthami N.M[3], Mahathi V[4], Mohan R[5]

[1]Asst. Professor, Electrical & Electronics, RajaRajeswari College Of Engineering
[2,3,4,5]UG Students, Electrical & Electronics, RajaRajeswari College Of Engineering

Abstract
The Aadhaar-Based Secure Voting System is designed to uphold the democratic principle of "one person, one vote" by implementing strong biometric authentication through Aadhaar data. The system integrates voter verification, secure vote casting, and an administrator dashboard for real-time monitoring. Core functionalities include duplicate and fraudulent vote prevention, migrated voter detection, and instant activity tracking. The architecture combines hardware components such as a fingerprint sensor, ESP8266 module, and LCD display with software technologies including SQLite for secure data storage, Streamlit for dashboard visualization, Pandas for data processing, and Matplotlib for real-time graphical analytics. The proposed solution enhances election security, transparency, and operational efficiency while providing administrators with comprehensive oversight. With its scalable design, the system has the potential for nationwide adoption. Future enhancements such as blockchain integration can further ensure immutability and end-to-end tamper-proof voting, strengthening democratic trust and reliability.

Keywords: Aadhaar Authentication; Biometric Voting; Secure Electronic Voting System; Fraud Prevention; Real-Time Monitoring; SQLite Database; ESP8266; Streamlit Dashboard; Election Transparency; Blockchain Integration; Digital Democracy.

1. INTRODUCTION

The Aadhaar-Based Secure Voting System modernizes traditional election processes by integrating biometric authentication, secure data handling, and real-time monitoring into a unified digital platform. The system uses Aadhaar-linked fingerprint verification to ensure that only genuine voters participate and that each individual votes exactly once, strengthening the core democratic principle of fair and transparent elections. With a combination of hardware components such as the fingerprint sensor, ESP8266 module, and LCD display, along with software elements including SQLite, Streamlit, Pandas, and Matplotlib, the system ensures secure storage, accurate processing, and continuous analysis of voter information.

A live administrative dashboard provides election officials with real-time visibility of the entire voting process, allowing them to track voter turnout, system activity, and potential anomalies instantly. This includes automated detection of migrated voters, prevention of duplicate or fake entries, and continuous data integrity checks to eliminate fraudulent attempts.The integration of analytical tools enables meaningful insights that support better decision-making and improve operational efficiency. The integration of analytical tools enables meaningful insights that support better decision-making and improve operational efficiency.

By bringing together multiple functional modules, the system enhances user experience for voters while increasing administrative control for officials. It promotes accessibility, transparency, and efficiency across the voting lifecycle, ensuring that every vote is handled securely from authentication to final counting.

2. Problem Statement

Traditional voting systems continue to face critical challenges such as impersonation, duplicate voting, lack of migrated voter support, and absence of real-time fraud detection. Manual identity verification is slow, error-prone, and vulnerable to manipulation, leading to reduced trust in the accuracy and fairness of election results. Existing digital voting models also lack strong biometric authentication and do not provide continuous monitoring or instant fraud alerts. Therefore, there is a need for a secure, Aadhaar-authenticated, biometric-based voting system that can verify voter identity accurately, prevent fraudulent activities, support migrated voters, and provide real-time transparency through automated monitoring and data analytics.

3. Literature review

Several research studies have explored secure electronic voting using biometrics, IoT, and Aadhaar authentication. Gupta and Sharma (2019) introduced an IoT-enabled e-voting model that focused on real-time monitoring and secure data handling. Patel and Bhavsar (2020) presented a blockchain-based e-voting framework that ensured transparency and tamper-proof vote recording. Singh and Kumar (2020) developed an Aadhaar and IoT-based smart voting system capable of detecting fraud and providing live monitoring. Balaji Naiak (2021) emphasized improving overall election integrity using fingerprint-based Aadhaar authentication.

Further advancements include the work of Holkar and Marab (2022), who proposed an IoT-driven biometric voting system to prevent proxy voting and enable real-time malfunction detection. Varma and Vantmure (2023) suggested linking Aadhaar and PAN-based biometric verification to eliminate fake voters and enhance system security. Gowtham et al. (2024) introduced a smart Aadhaar-linked voting system that allowed voters to cast ballots from any location. Nandhakumar (2024) implemented fingerprint authentication with IoT to prevent duplicate voting and ensure secure identification. Most recently, Satyanarayana and Pranam (2025) developed a biometric-based electronic voting system using fingerprint sensors and SQLite to secure data and reduce voter fraud.

4. Existing System

The current voting system relies on manual verification and basic EVMs without biometric authentication.

It is vulnerable to impersonation, duplicate voting, and proxy voting. Migrated voters face difficulty voting from new locations. There is no real-time fraud detection or monitoring. Data storage is not fully secure and can be manipulated. Counting and verification are slow and prone to human error. Overall, the system lacks transparency, security, and accuracy.

5. Proposed System

The proposed system introduces Aadhaar-based fingerprint authentication to verify the voter's identity

with high accuracy. It eliminates duplicate, fake, and proxy voting by ensuring that each voter can vote only once. The fingerprint sensor and NodeMCU authenticate voters in real time before allowing access to the voting interface. A migrated voter support mechanism enables voters to cast their vote securely from any registered location. Fraud attempts, mismatches, and unauthorized access are instantly detected and recorded in the database. All authenticated votes are securely transmitted to the server through IoT-based communication. A Streamlit-based live dashboard displays real-time voting activity, fraud alerts, turnout statistics, and system status. The SQLite database ensures safe storage of voter data and voting logs without tampering. The overall system significantly enhances election reliability by combining biometric security, IoT connectivity, and real-time monitoring into a single integrated framework.
In addition, the system reduces human intervention, minimizing manual errors and delays. The modular design makes it easy to scale for larger elections and adapt to different institutions. Overall, the system ensures transparency, accessibility, and high security throughout the voting process.

6. Methodology

The methodology follows a structured process beginning with Aadhaar-based voter registration, where each voter's fingerprint is securely stored in the SQLite database. During voting, the R307 fingerprint sensor captures the voter's biometric data, and the NodeMCU ESP8266 validates it against stored records. If authentication is successful, the
system enables the voter to select a candidate using push buttons. Fraud attempts such as duplicate or mismatched fingerprints trigger immediate alerts displayed on the LCD and recorded in the database. The verified voting data is transmitted through a secure Wi-Fi channel to the Flask server. Finally, the Streamlit dashboard displays real-time voting activity, fraud alerts, and turnout analytics, ensuring transparency and continuous monitoring throughout the election process.

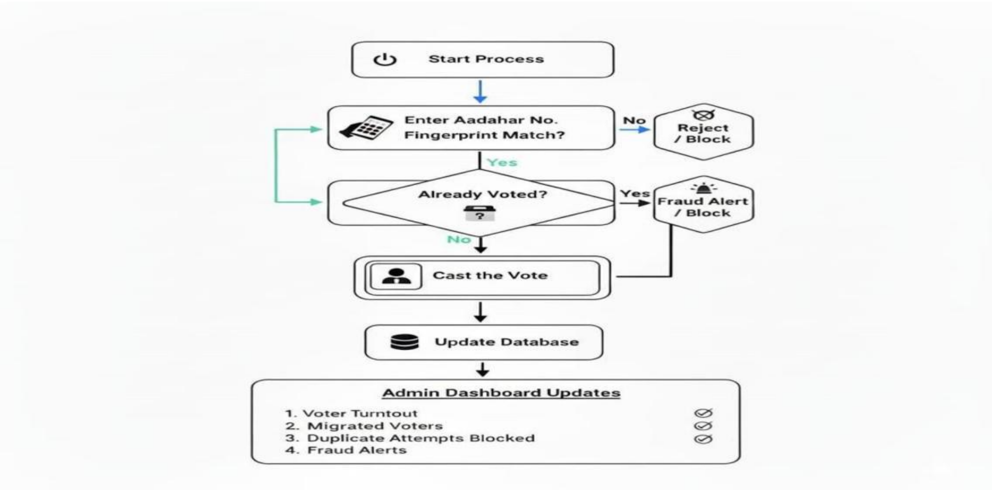

Figure 1: Flow Chart

The flowchart begins with the voter approaching the voting module and placing their finger on the fingerprint sensor. The captured biometric data is compared with Aadhaar-linked records stored in the database. If the fingerprint does not match or if a duplicate attempt is detected, the system activates a fraud alert and blocks access. If the fingerprint verification is successful, the system enables the voting interface where the voter selects their preferred candidate. The vote is recorded and securely sent to the server, which updates the database. Simultaneously, the real-time dashboard displays the vote count, authentication logs, and any fraud events. The process ends after the vote is successfully stored and displayed for monitoring.

System Architecture

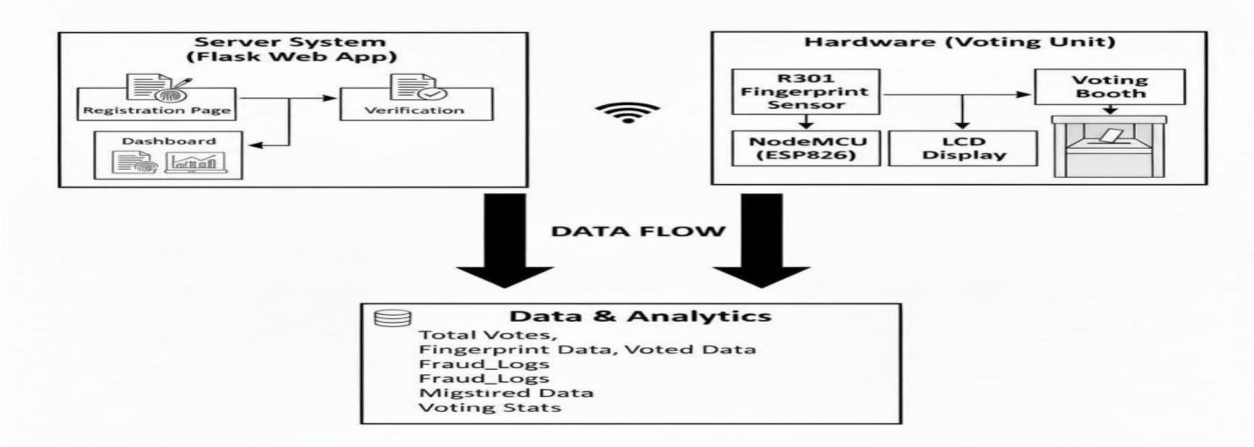

Figure 2: Block Diagram

The proposed Aadhaar-Based Fraud-Resistant Voting System is designed using interconnected hardware and software components that work together to ensure secure, authenticated, and transparent voting.

1. **Microcontroller (Central Processing Unit – The Brain)**

- **NodeMCU ESP8266:**

Acts as the core controller of the system. It communicates with all input devices, processes fingerprint authentication, handles vote selection, and transmits verified data to the server through Wi-Fi. The ESP8266 enables real-time data exchange, making the system fully IoT-enabled.

2. **Input Units (User Identification & Vote Selection)**

- **R307 Fingerprint Sensor:**
  Captures the voter's fingerprint and matches it with Aadhaar-linked biometric data stored in the database. Ensures only registered and genuine voters can vote.
- **Push Buttons (Candidate Selection):**
  After successful verification, the voter chooses their preferred candidate through dedicated push buttons. Each button corresponds to a candidate or voting option.

3. **Output Modules (User Guidance & Status Display)**

- **16x2 LCD Display:**
  Shows real-time system messages such as "Place Finger," "Verifying…," "Verified," "Vote Recorded," or "Fraud Detected." Guides the user through each step of the process.

4. **Communication & Data Transfer (IoT Module)**

- **Wi-Fi Communication (ESP8266):**
  Securely sends authenticated voter IDs, vote data, and fraud alerts to the Flask server.
  Ensures seamless, low-latency data transfer for real-time monitoring.

5. **Server-Side Processing (Backend Logic)**

- **Flask (app.py):**

Handles all backend operations including voter verification, vote logging, fraud detection, and database communication.

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Manages API routes for the dashboard to fetch real-time updates**.**

- **SQLite Database:**

Serves as the secure storage system for Aadhaar data, fingerprints, fraud logs, vote counts, and migrated voter information.

Ensures tamper-resistant, fast-access data management.

6. **Monitoring & Analytics (Admin Dashboard).**

- **Streamlit Dashboard:**
  Provides a live visualization of voting activity including: Real-time turnout, Fraud attempts, Authentication logs, Vote count analytics, System health status
  This dashboard supports administrators with instant decision-making and complete transparency.

7. **Security & Fraud Prevention Layer**

- Real-time biometric verification ensures one-voter-one-vote.
- Duplicate or mismatched fingerprints trigger immediate alerts.
- Every activity (login, vote, fraud attempt) is recorded in the server logs.
- Ensures transparency, security, and zero unauthorized access.

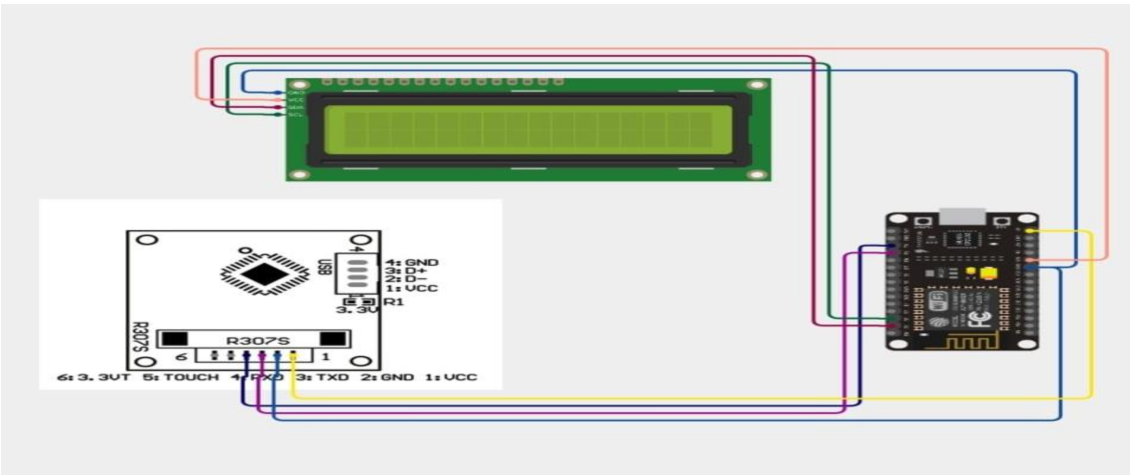

Figure 3: Circuit Diagram

7. **Hardware & Software Components**

The hardware of the proposed system consists of the NodeMCU ESP8266, which functions as the main controller responsible for processing all inputs and handling communication with the server. The R307 fingerprint sensor serves as the primary biometric input device, capturing and verifying the voter's fingerprint. An LCD display provides real-time feedback to the user by showing messages such as verification status and fraud alerts, while push buttons allow voters to select their preferred candidate after successful authentication. A stable power supply supports continuous and reliable operation of all modules.

The software components include Python, which is used to develop the backend logic of the system, and the Flask framework (app.py), which manages routes for user authentication, vote recording, and fraud detection. SQLite is used as the database for securely storing voter information, fingerprints, votes, and system logs. The Streamlit dashboard provides real-time monitoring and visualization of voting activities, including voter turnout and fraud attempts. Additionally, Pandas and Matplotlib are utilized

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

for data processing and generating analytical graphs that enhance administrative decision-making.

8. Result

The developed Aadhaar-Based Secure Voting System was implemented successfully and tested using a functional web interface integrated with biometric verification. The system allows users to register, verify fingerprints, and cast their vote securely. During testing, the platform showed reliable performance in detecting mismatched fingerprints, preventing duplicate voting, and supporting migrated voters.

The registration module accurately captured Aadhaar details, city, and fingerprint data. The verification module responded correctly to both successful and failed fingerprint matches, displaying clear visual alerts. The migrated voter feature worked as expected by allowing users to vote from a different city while updating the dashboard in real time. The voting module allowed casting exactly one vote and immediately locked further access after submission. Overall, the results demonstrate that the system is stable, user-friendly, and highly effective in ensuring secure and authenticated voting.

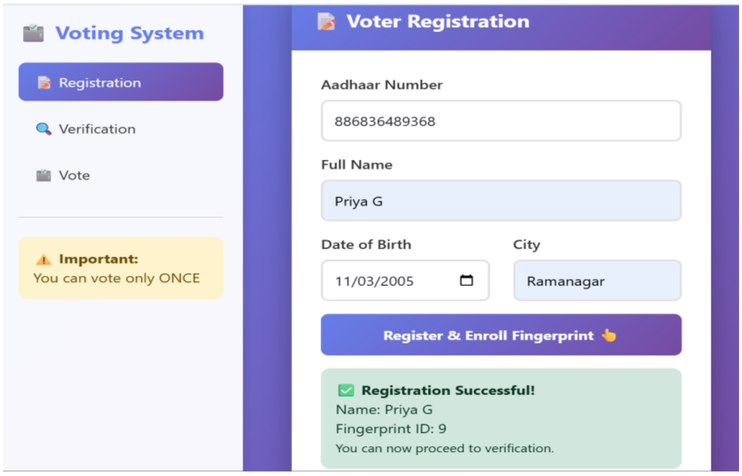

Figure 4: Registration Success Screen

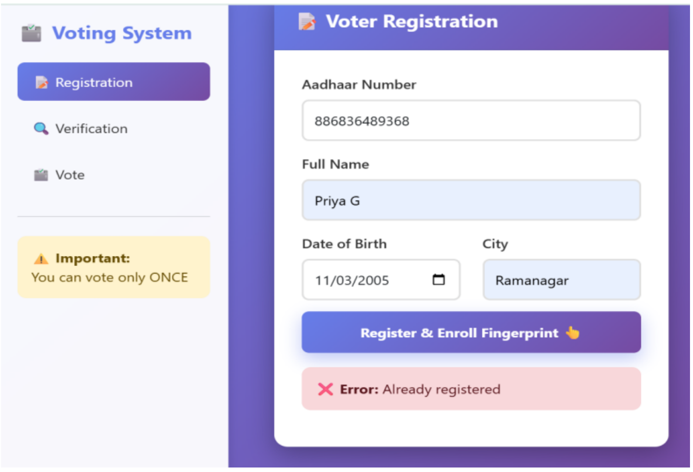

Figure 5: Duplicate Registration Alert

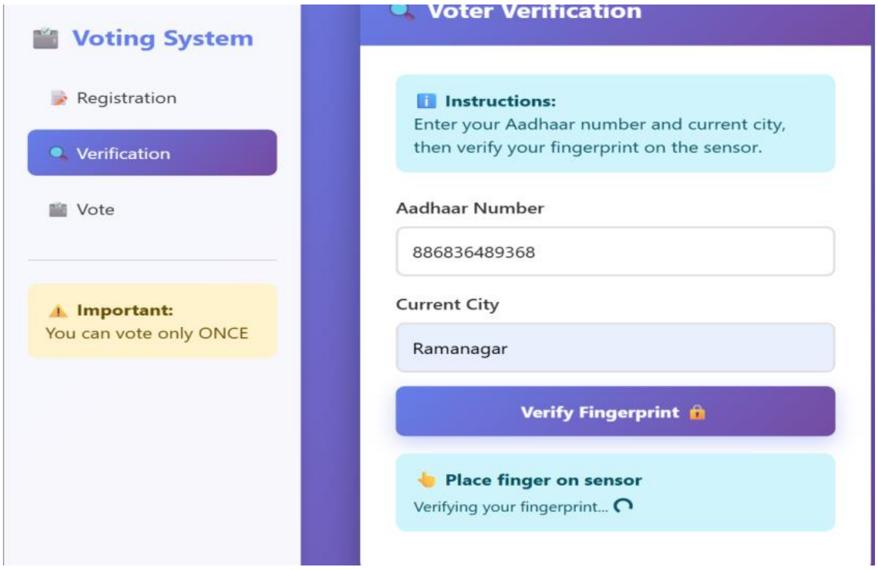

Figure 6: Local Voter Verification Screen

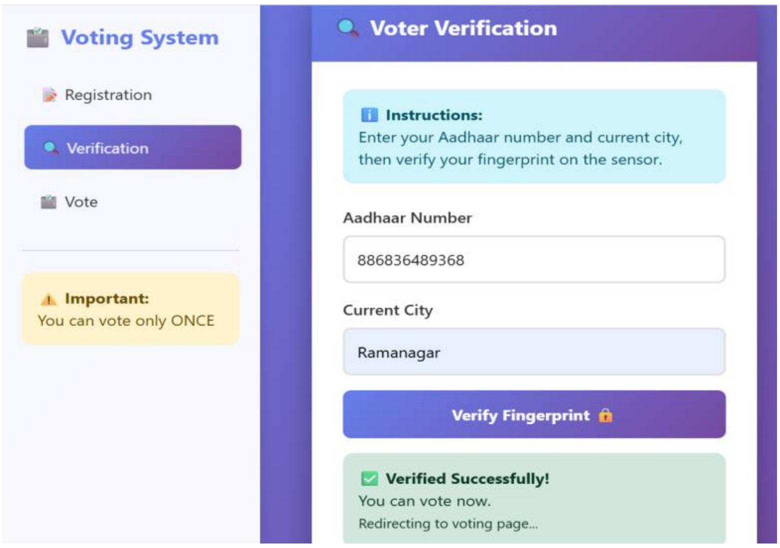

Figure 7: Verification Successful Screen

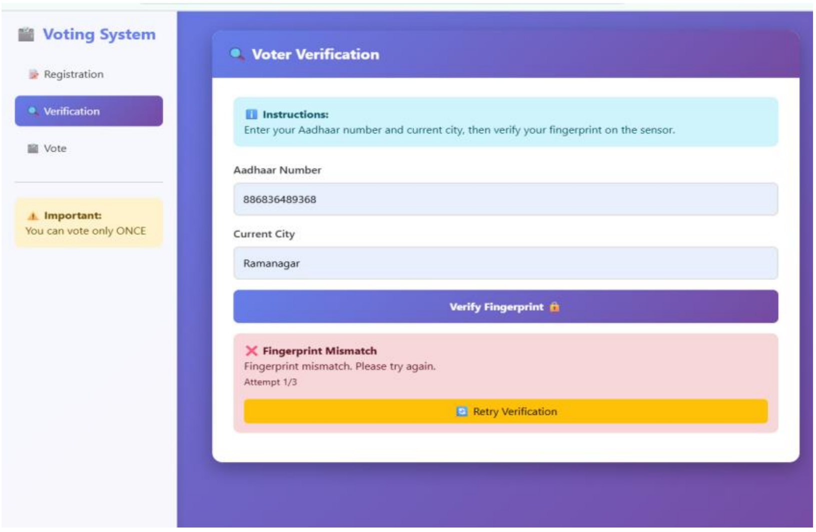

Figure 8: Fingerprint Mismatch Warning

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

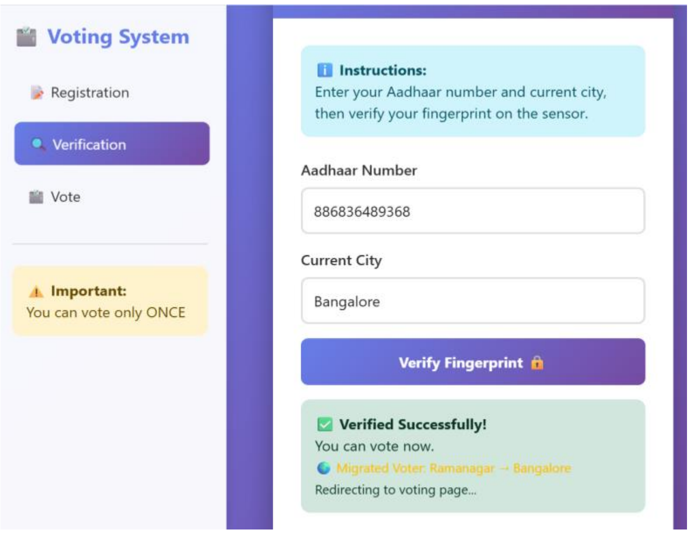

Figure 9: Migrated Voter Detected Screen

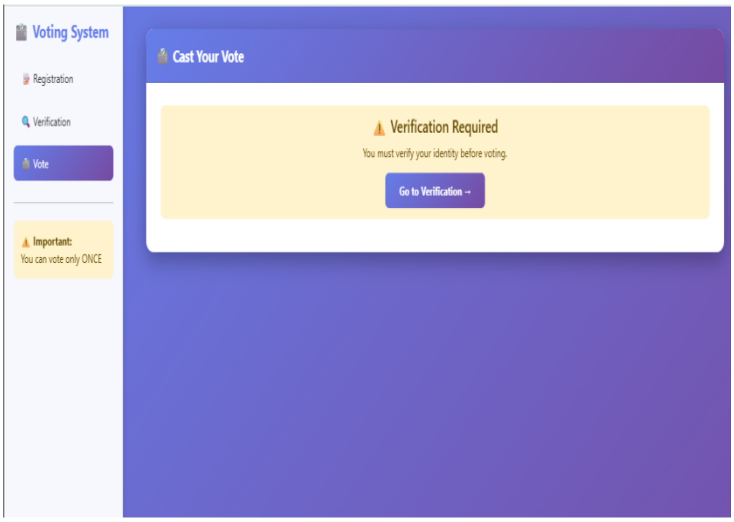

Figure 10. Vote Selection Page

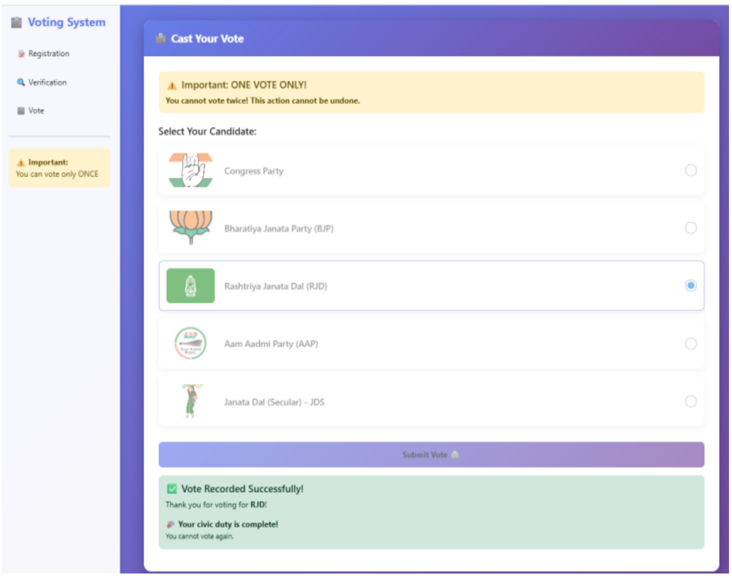

Figure 11: Vote Submission Confirmation

International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

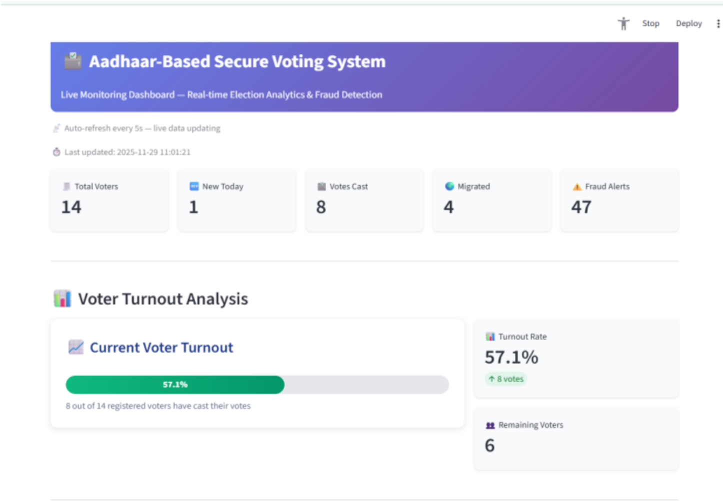

Figure 12: Live Voting Dashboard

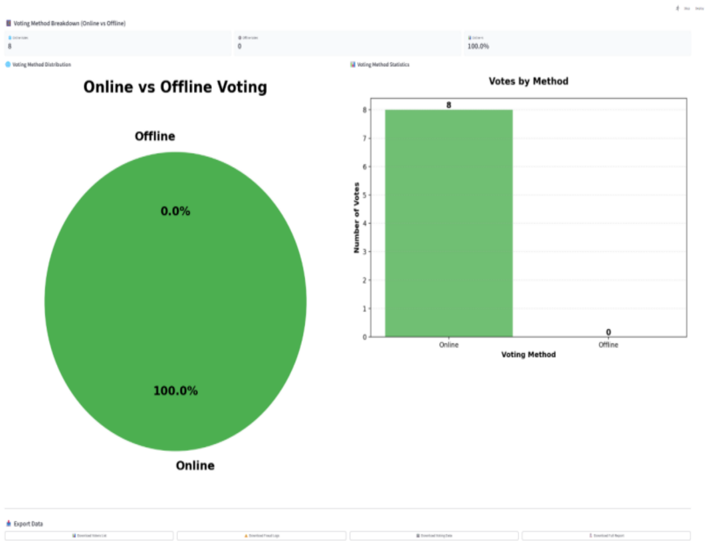

Figure 13: Fraud Detection Dashboard

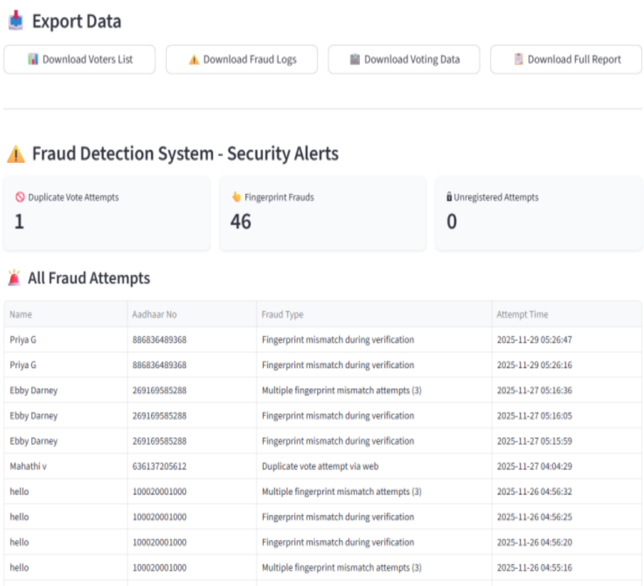

Figure 14: Authentication Log Dashboard

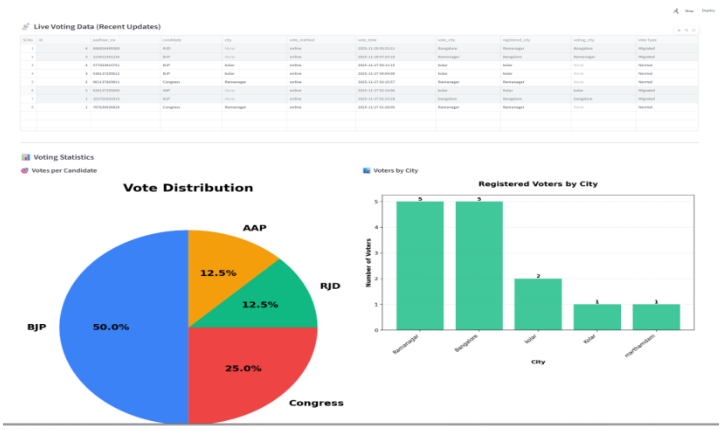

Figure 15: Vote Count Statistics Dashboard

Figure 16: Hardware set up

9. Discussion

The implementation and testing of the Aadhaar-Based Secure Voting System demonstrate that biometric authentication significantly enhances the accuracy and integrity of vote casting. The integration of fingerprint verification ensures that only genuine registered voters participate, while the one-vote-only rule prevents duplication and impersonation. The system also successfully supports migrated voters by allowing verification and voting from a different location, thereby improving accessibility.

Real-time communication between the ESP8266 microcontroller and the server ensures fast authentication and immediate fraud detection. The Streamlit admin dashboard provides continuous monitoring, making election oversight transparent and efficient. Although the prototype performs reliably, further improvements such as advanced encryption, large-scale database management, and multi-biometric verification can strengthen performance in real-world nationwide deployment.

10. Conclusion

The proposed Aadhaar-Based Secure Voting System successfully addresses critical challenges in traditional voting, such as impersonation, duplicate voting, fake entries, and lack of real-time monitoring. By integrating fingerprint authentication, IoT communication, secure data storage, and a live monitoring dashboard, the system ensures transparency, accuracy, and enhanced voter trust. The prototype validates that biometric-based verification combined with digital monitoring offers a strong foundation for a secure and reliable e-voting framework. This work contributes toward modernizing the electoral process and demonstrates that Aadhaar-linked biometric verification can support scalable, tamper-resistant, and accessible voting solutions.

10. Acknowledgment

We would like to express our sincere gratitude to **Prof. Sweatha R** for her continuous guidance, valuable suggestions, and encouragement throughout the project.

We also thank **Dr. Arul Josh** for his technical support and timely assistance, which greatly contributed to the successful completion of this work.

Finally, we appreciate the cooperation and contributions of all project team members who worked together to complete this research effectively.

11. Reference

1. Agarwal, M., & Srivastava, R. “Biometric Fingerprint Recognition for Secure Electronic Voting”, International Journal of Computer Applications, 2023.
2. Patil, S., & Kulkarni, D., “IoT-Enabled Smart Voting Machine with Aadhaar Verification”, IEEE International Conference on Communication and Electronics Systems (ICCES), 2024.
3. Hossain, A., & Rahman, M., “Cloud-Based Electronic Voting with Fingerprint Authentication”, Journal of Network and Computer Applications, 2024.
4. Deshmukh, A., & Dey, P., “A Secure E-Voting Architecture Using Blockchain and Biometrics”, IEEE Access, 2025.
5. Ahmed, T., & Kumar, N., “AI-Driven Fraud Detection in Biometric Voting Systems”, ACM Transactions on Information and System Security (TISSEC), 2025.
6. Li, X., & Zhang, Y., "Transforming Online Voting: Blockchain and Biometric Verification for Enhanced Security," Cluster Computing, 2019.
7. Sharma, P., & Rao, V., “Secure Electronic Voting System Using Biometric Authentication,” IEEE Transactions on Information Forensics and Security, 2020.
8. Singh, R., & Mehta, K., “Real-Time Dashboard for Monitoring Electronic Voting Process Using IoT,” IEEE Internet of Things Journal, 2020.
9. Kumar, S., & Gupta, A., "Design and Implementation of Blockchain-Based E-Voting System," IEEE International Conference on Smart Computing, Bengaluru, 2021.
10. Zhang, Y., & Wang, X., "Secured E-Voting System Based on Iris Identification," International Conference on Computer Science and Information Technology, 2022.