IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

IoT-Based Secure EVM (Electronic Voting Machine) with Biometric and OTP Verification, Offline Result Storage, and Live Web Display

Gunjal Ayush Kiran, Shinde Shraddha Vijaykumar, Nagare Siddhi Rajendra, Chaudhari Sahil Jagdish, Dr. R. S. Pawase
Department of Electronics and Telecommunication Engineering.
Amrutvahini College of Engineering, Sangamner

Abstract: *The IoT-Based Secure Electronic Voting Machine (EVM) is designed to provide a secure, transparent, and efficient voting system using biometric fingerprint authentication and OTP verification. The ESP32 microcontroller acts as the main control unit, managing voter verification, vote recording, and communication processes. After successful authentication, voters can cast their votes through push buttons, and the results are stored both offline using an and online through IoT-based live web display. The system minimizes duplicate voting, enhances election security, and ensures reliable data storage with real-time monitoring capabilities. This project offers a modern and user-friendly solution suitable for institutional and small-scale election applications*

Keywords: IoT-Based EVM, ESP32 Microcontroller, Fingerprint Authentication, OTP Verification, GSM Module,Storage, Real-Time Web Display, Electronic Voting System, Biometric Security, IoT Technology

I. INTRODUCTION

Electronic Voting Machines (EVMs) have become an important part of modern election systems because they reduce manual errors, speed up vote counting, and simplify the voting process. However, traditional EVMs still face several security challenges such as duplicate voting, voter impersonation, unauthorized access, and data tampering [1]. To overcome these issues, advanced technologies such as biometric authentication, OTP verification, and IoT-based monitoring are being integrated into electronic voting systems [2].

The proposed IoT-Based Secure Electronic Voting Machine uses the ESP32 microcontroller as the central processing unit for controlling authentication, vote recording, and communication functions [3]. The system uses a fingerprint sensor for biometric voter identification and a GSM module for sending One-Time Passwords (OTP) to registered users, providing dual-layer security [4]. This approach increases the reliability and transparency of the voting process while preventing fake or duplicate voting [5].

After successful verification, voters can cast their votes using push-button switches connected to the controller. The recorded voting data is stored locally on an for offline backup and simultaneously uploaded to a cloud server for live web-based result display [6]. This dual-storage mechanism improves data reliability and ensures that voting records remain safe even during network failures [7].

The integration of IoT technology enables real-time monitoring and transparent result declaration through a web interface [8]. The LCD display and buzzer guide the voter throughout the process by providing instructions and confirmation messages [9]. Overall, the proposed system provides a secure, efficient, and user-friendly voting solution suitable for schools, organizations, and small-scale government elections [10].

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

II. PROBLEM STATEMENT

Traditional Electronic Voting Machines (EVMs) are widely used for conducting elections, but they still face several challenges related to security, transparency, and data reliability. Issues such as duplicate voting, voter impersonation, unauthorized access, manual errors, and lack of secure result monitoring reduce the trustworthiness of the voting process. In many existing systems, the absence of multi-level authentication and proper backup mechanisms increases the risk of vote tampering and data loss during network or power failures. Therefore, there is a need to develop a secure and efficient IoT-based Electronic Voting Machine that uses biometric fingerprint authentication and OTP verification to ensure genuine voter identification, while also providing offline data storage and real-time web-based result monitoring for improved transparency, reliability, and election integrity.

III. OBJECTIVES

1. To develop a secure Electronic Voting Machine using the ESP32 microcontroller and IoT technology.
2. To verify voter identity using fingerprint-based biometric authentication.
3. To implement OTP verification for providing an additional layer of voting security.
4. To store voting data securely in both offline storage and online cloud platforms.
5. To display election results in real time through a live web-based monitoring system.

IV. LITERATURE SURVEY

Shaikh Tazaeen Ilyas et al. (2022) presented a biometric-based secured electronic voting system in the International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET). The study discussed the use of fingerprint, iris, and facial recognition techniques for voter authentication in electronic voting systems. The authors highlighted that biometric verification improves security and reduces fake voting. However, the system faced challenges related to biometric data protection and network dependency.

Bhatti Jasdev et al. (2019) developed a secure electronic voting machine using multi-modal biometric authentication and encryption techniques. Their system combined fingerprint and facial recognition with secure data transmission methods to prevent tampering and unauthorized access. The proposed method improved election security but increased system complexity and hardware cost.

Roy Arnab et al. (2023) proposed an online voting system using face recognition and One-Time Password (OTP) verification. The system authenticated voters using facial recognition and sent OTPs to registered mobile numbers for additional security. Their approach minimized unauthorized voting and improved reliability, but it depended heavily on internet connectivity and server availability.

Kumar R. and Prasad N. (2022) introduced an IoT-based fingerprint voting machine that used biometric authentication and cloud connectivity for secure vote management. The system allowed real-time result monitoring through IoT integration and ensured that each voter could vote only once. However, network failure could affect continuous data synchronization.

Verma P. and Yadav R. (2021) designed an IoT-based advanced electronic voting system using low-cost embedded devices and cloud storage. Their system provided dual data storage through local memory and online cloud backup, improving data reliability and transparency. The study concluded that IoT technology can significantly modernize voting systems, though security against cyberattacks remained a concern.

Pushpavalli K. et al. (2025) proposed a secure electronic voting system with fingerprint authentication and OTP verification for enhanced voter security. The system used biometric verification to confirm voter identity and GSM-based OTP generation for two-factor authentication.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, May 2026 Impact Factor: 8.2

Comparison Table

Author & Year	Method Used	Advantages	Limitation s
Shaikh Tazaeen Ilyas et al. (2022)	Biometric-based E-voting using fingerprint and facial recognition	Improved voter authenticatio n and reduced fake voting	Biometric data security issues
Bhatti Jasdev et al. (2019)	Multi-modal biometric authentication with encryption	High security and secure data transmission	Complex system design
Roy Arnab et al. (2023)	Face recognition with OTP verification	Prevented unauthorized voting	Dependent on internet connectivit y
Kumar R. and Prasad N. (2022)	IoT-based fingerprint voting machine	Real-time monitoring and secure voting	Network dependency
Verma P. and Yadav R. (2021)	IoT-based EVM with cloud and local storage	Data backup and transparency	Vulnerable to cyber threats
Pushpavall i K. et al. (2025)	Fingerprint and OTP-based secure voting system	Dual-layer security and reliable authentication	OTP delay in weak networks

IV. WORKING OF SYSTEM

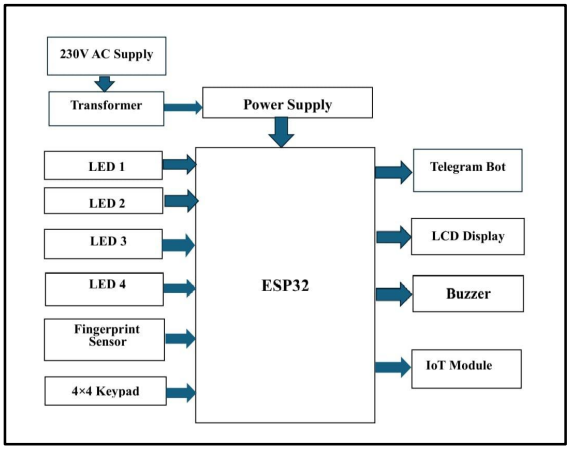

Fig 1: Design of the system

1. Power Supply Initialization

The system operates using a 230V AC power supply, which is converted into the required DC voltage through a transformer and regulated power supply circuit. This provides stable power to the ESP32 microcontroller and all connected modules for smooth operation of the voting system.

2. ESP32 as Central Controller

The ESP32 microcontroller acts as the main processing and control unit of the system. It manages communication between the fingerprint sensor, keypad, LEDs, LCD display, buzzer, Telegram Bot, and IoT module. It also processes voter authentication, vote recording, and online result updates.

3. Fingerprint Authentication

When a voter starts the voting process, the fingerprint sensor scans the voter's fingerprint. The ESP32 compares the scanned fingerprint with the stored database templates. If the fingerprint matches, the voter is authenticated successfully and allowed to proceed to the next verification step.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, May 2026 Impact Factor: 8.2

4. OTP Verification through Telegram Bot

After successful fingerprint verification, the ESP32 sends a One-Time Password (OTP) to the voter through the Telegram Bot platform. The voter enters the received OTP using the 4×4 keypad. The ESP32 verifies the entered OTP to ensure secure and genuine voter authentication.

5. Candidate Selection Using LEDs and Buttons

Once the OTP is verified, the voting panel becomes active. The voter selects the preferred candidate by pressing the corresponding voting button associated with LED indicators (LED1 to LED4). The selected LED glows to indicate successful vote selection.

6. Vote Confirmation through Buzzer and LCD

After the vote is cast successfully, the buzzer produces a beep sound as confirmation. Simultaneously, the LCD display shows messages such as "Vote Recorded Successfully" or "Thank You for Voting," guiding the voter throughout the process.

7. Data Storage and IoT Monitoring

The ESP32 records the voting data and sends it to the IoT module for real-time online monitoring and live result display. This enables transparent result tracking through a web interface or cloud platform. The system can also maintain offline backup storage for additional reliability.

8. System Reset for Next Voter

After completing the voting process, the system automatically resets itself and becomes ready for the next voter. This ensures continuous, secure, and efficient operation during the election process.

V. SYSTEM DESIGN

1. Power Supply Unit

The power supply unit converts AC voltage into regulated DC voltage required for the operation of the ESP32 and all connected electronic components. It ensures stable and uninterrupted power for smooth system performance.

2. ESP32 Microcontroller

The ESP32 acts as the main control unit of the system. It manages voter authentication, OTP verification, vote recording, LCD display messages, buzzer indications, and IoT communication for live result monitoring.

3. Fingerprint Sensor Module

Fig.2.Fingerprint Sensor

The fingerprint sensor is used for biometric authentication of voters. It scans and verifies the fingerprint of the voter with stored templates to ensure that only authorized users can access the voting system.

4. OTP Verification System

After successful fingerprint authentication, the ESP32 generates and sends an OTP to the voter using the Telegram Bot or GSM module. The OTP provides an additional security layer to prevent unauthorized voting.

5. 4×4 Keypad Interface

The keypad allows the voter to enter the received OTP into the system. It serves as an input device for secure interaction between the user and the voting machine.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 8, May 2026
Impact Factor: 8.2

6. Voting Panel with LED Indicators

The voting section contains push buttons and LED indicators representing different candidates. The voter presses the corresponding button to cast a vote, and the LED glows to confirm the selected candidate.

7. LCD Display Module

The LCD display provides step-by-step instructions and status messages such as “Place Finger,” “Enter OTP,” and “Vote Recorded Successfully.” It improves user interaction and reduces operational errors.

8. Buzzer Unit

Fig.3.Buzzer Unit

The buzzer generates audio alerts during different stages of the voting process. It confirms successful authentication and vote submission while also indicating errors or invalid operations.

9. IoT Communication Module

The IoT module enables real-time transmission of voting data to a cloud server or web dashboard. This allows live monitoring and transparent display of election results through internet connectivity.

10. Data Storage System

The system securely stores voting records for future verification and backup purposes. Both online and offline storage methods can be used to ensure data reliability and prevent data loss.

VI. RESULTS

Fig.4.Prototype Model

The developed IoT-Based Secure Electronic Voting Machine successfully performed secure and reliable electronic voting using biometric fingerprint authentication and OTP verification. The ESP32 microcontroller effectively controlled all system operations, including voter authentication, vote processing, and IoT communication. During

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, May 2026 Impact Factor: 8.2

testing, the fingerprint sensor accurately identified registered voters and prevented unauthorized access or duplicate voting attempts. After successful fingerprint matching, OTP verification through the Telegram Bot provided an additional layer of security, ensuring that only genuine users could cast votes.

The LCD display guided users throughout the voting process by displaying clear instructions and status messages, while the buzzer provided confirmation alerts after successful vote submission. The voting buttons and LED indicators operated correctly, allowing voters to easily select their preferred candidates. The system also demonstrated successful real-time data transmission through the IoT module, enabling live result monitoring and transparent vote counting through the web interface.

Furthermore, the system maintained reliable vote storage and data handling throughout operation. All votes were recorded accurately without data loss, even during repeated testing cycles. The overall performance of the proposed system proved that the integration of biometric authentication, OTP verification, and IoT technology can significantly improve the security, transparency, and efficiency of electronic voting systems for institutional and small-scale election applications.

VII. CONCLUSION

The IoT-Based Secure Electronic Voting Machine provides a reliable, secure, and transparent solution for modern electronic voting applications. The integration of fingerprint authentication and OTP verification ensures that only authorized voters can cast their votes, thereby reducing the chances of duplicate or fake voting. The ESP32 microcontroller efficiently manages all system operations, including authentication, vote recording, and IoT communication. The system also enables real-time result monitoring through web-based connectivity while maintaining secure data storage for improved reliability. The LCD display, buzzer, and voting panel provide a simple and user-friendly interface for voters. Overall, the proposed system successfully improves election security, transparency, and efficiency, making it suitable for schools, organizations, and small-scale election environments.

VIII. FUTURE SCOPE

The proposed IoT-Based Secure Electronic Voting Machine can be further improved by integrating advanced technologies to enhance security, reliability, and scalability. Future versions of the system may include additional biometric authentication methods such as face recognition or iris scanning for stronger voter verification. Blockchain technology can also be implemented to provide tamper-proof vote storage and improve transparency in election processes. The system can be expanded with cloud database integration and mobile application support to enable secure remote voting and centralized election monitoring. Artificial Intelligence (AI) techniques may be used to detect suspicious activities and prevent fraudulent voting attempts automatically. Furthermore, multilingual user interfaces, larger voter database capacity, and renewable power backup systems such as solar energy can make the system more suitable for large-scale government and public elections.

REFERENCES

[1] S. Gurav, A. Fase, D. Masal, and K. I. Chouhan, “Fingerprint Based Voting System Using IoT,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), vol. 10, no. 6, pp. 888–894, 2024.

[2] A. M. Jagtap, V. Kesarkar, and A. Supekar, “Electronic Voting System using Biometrics, Raspberry Pi and TFT Module,” in International Conference on Advanced Computing and Communication Systems, 2019, pp. 112–116.

[3] S. M. Hasan, A. M. Anis, H. Rahman, J. S. Alam, S. I. Nabil, and M. K. Rahman, “Development of Electronic Voting Machine with Near Field Communication ID Cards and Biometric Fingerprint Identifier,” in 17th International Conference on Computer and Information Technology (ICCIT), 2014, pp. 383–387.

[4] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, “Biometric Based Secured Remote Electronic Voting System,” in IEEE 7th International Conference on Smart Structures and Systems (ICSSS), 2020, pp. 1–5.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 8, May 2026 Impact Factor: 8.2

[5] M. A. Zamir, D. A. Khan, and M. S. Umar, "Secure Electronic Voting Machine Using Biometric Authentication," International Journal of Advanced Research in Computer Science, vol. 9, no. 2, pp. 45–50, 2018.
[6] R. Kumar and N. Prasad, "Fingerprint Biometric Voting Machine Using Internet of Things (IoT)," International Journal of Computer Applications, vol. 184, no. 12, pp. 15–20, 2022.
[7] P. Verma and R. Yadav, "IoT-Based Advanced Voting Machine System Enhanced Using Low-Cost Embedded Devices and Cloud Platform," International Journal of Engineering Trends and Technology (IJETT), vol. 69, no. 5, pp. 101–107, 2021.
[8] K. Pushpavalli, R. Meena, and S. Priya, "Secure E-Voting System with Biometric Authentication," in Proceedings of the International Conference on Emerging Trends in Engineering and Technology, Atlantis Press, 2025, pp. 210–216.
[9] S. C. Venugopal and R. K. Rajan, "IoT-Based Voting Machine with Fingerprint Verification," International Journal of Research in Engineering and Science (IJRES), vol. 9, no. 5, pp. 25–31, 2022.
[10] A. Mishra and D. Gupta, "IoT-Based Advanced E-Voting System for Transparent Elections," International Journal of Recent Technology and Engineering (IJRTE), vol. 11, no. 3, pp. 55–61, 2023.
[11] T. Ilyas, S. Gugale, H. Ranadhir, V. Patil, and O. Kulkarni, "A Survey on Biometrics Based Secured E-Voting System," International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), vol. 9, no. 3, pp. 122–128, 2022.
[12] J. Bhatti, S. Chachra, A. Walia, and V. Abhishek, "Secure Electronic Voting Machine using Multi-Modal Biometric Authentication System, Data Encryption, and Firewall," International Journal of Performability Engineering, vol. 15, no. 10, pp. 2715–2723, 2019.
[13] A. Roy, D. Sharma, M. Verma, A. Singh, and R. P. Pawar, "Online Voting System Using Face Recognition and One-Time Password," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 11, no. 4, pp. 1020–1026, 2023.
[14] N. Deshmukh and P. Joshi, "Blockchain-Based Voting for Transparent Elections," IEEE Access, vol. 8, pp. 215–223, 2020.
[15] L. Patel and A. Kumar, "Real-Time Voting Using IoT and Web Integration," International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 7, pp. 340–345, 2021.
[16] S. Thomas and R. George, "Secure E-Voting System Using Fingerprint and Aadhaar Verification," International Research Journal of Engineering and Technology (IRJET), vol. 9, no. 6, pp. 450–456, 2022.
[17] T. Banerjee and P. Sinha, "Dual Authentication Voting Machine Using IoT," International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 11, no. 5, pp. 789–795, 2023.
[18] A. Sharma and M. Jain, "Electronic Voting System Using Raspberry Pi and Python," International Journal of Advance Engineering and Research Development (IJAERD), vol. 6, no. 4, pp. 155–160, 2019.
[19] J. Patel and R. Mehta, "E-Voting System with Cloud Database Using ESP32," International Journal of Engineering Trends and Technology (IJETT), vol. 70, no. 2, pp. 88–94, 2022.
[20] P. Roy and N. Das, "Enhanced E-Voting System with Encryption," Elsevier Procedia Computer Science, vol. 171, pp. 1450–1457, 2021