# International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2(1) (2026)



ijerst.editor@gmail.com

editor@ijerst.com

# Intelligent Digital Voting System Using ESP32 with Biometrics and Camera Based Authentication Framework

Vuppula Manohar[1*], Jaligama Naga Srinidh[2], Madagani Likitha[2], Ragi Shobhanbabu[2]

[1] Associate Professor & Head, [2]UG Student, [1,2]Department of Electronics & Communication Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

*Correspondence: Vuppula Manohar (manoharvu@gmail.com)

**Abstract**

The growing demand for secure and transparent electoral systems has intensified due to increasing concerns over election fraud, with reports indicating that digital and identity-based fraud impacts millions of voting processes globally, while e-governance and smart voting technologies are projected to grow at over 18% annually. These environments require tamper-proof mechanisms, efficient monitoring, and rapid fraud detection to ensure fairness and accuracy. Traditional voting systems, whether paper-based or basic electronic machines, are prone to issues such as identity fraud, vote manipulation, lack of transparency, and delayed result processing. Furthermore, conventional systems lack multi-layer authentication, real-time alerts, and centralized monitoring, making them vulnerable to unauthorized activities. To overcome these limitations, the proposed biometric and CAM based E-voting system utilizes the ESP32 microcontroller to implement a secure, IoT-enabled voting framework with predictive fraud prevention. The system integrates RFID authentication, fingerprint biometric verification, and camera-based monitoring to ensure multi-factor voter validation. A keypad-based interface allows users to cast votes, while an LCD provides real-time guidance and feedback. Suspicious activities such as unauthorized access or repeated attempts trigger buzzer alerts and instant SMS notifications via a GSM module, with all events logged on the IoT platform for analysis. Real-time vote updates and secure result dissemination enhance transparency, while a controlled polling switch ensures proper election closure. This intelligent system significantly improves election security, prevents fraud, and provides a reliable, scalable solution for modern digital voting systems.

**Keywords:** Biometric Authentication, Electronic Voting System, Fraud Detection, GSM Communication, Internet of Things, Secure Voting, Smart Governance, Voter Authentication

## 1. Introduction

The increasing demand for secure and transparent electoral systems has become a major global concern due to rising instances of election fraud and identity manipulation [1]. Reports indicate that millions of voting processes worldwide are affected by digital and identity-based fraud, undermining public trust in democratic systems. At the same time, the adoption of e-governance and smart voting technologies is growing rapidly, with projections exceeding 18% annual growth, driven by the need for efficient, transparent, and tamper-proof election mechanisms [2]. Modern electoral environments require systems capable of ensuring accurate voter authentication, real-time monitoring, and secure data handling to maintain fairness and integrity throughout the voting process [3].

Traditional voting systems, including paper-based ballots and basic electronic voting machines, are associated with several limitations. Paper-based systems are time-consuming [4], prone to human errors, and vulnerable to manipulation during counting and storage. Basic electronic systems, although faster, often lack robust security features and are susceptible to unauthorized

access and tampering [5]. Additionally, these systems typically rely on single-layer authentication methods, which can be bypassed through identity fraud or impersonation. The absence of real-time monitoring, alert mechanisms, and centralized data management further reduces transparency and makes it difficult to detect and prevent fraudulent activities during elections.

In real-time scenarios, these limitations result in critical challenges that compromise the credibility of the electoral process [6]. Identity fraud and duplicate voting can occur due to weak authentication mechanisms, while lack of continuous monitoring delays the detection of suspicious activities. The absence of immediate alerts and data logging prevents timely intervention, increasing the risk of vote manipulation [7]. Furthermore, delayed result processing and limited transparency reduce public confidence in election outcomes. These challenges highlight the necessity for an intelligent, IoT-enabled voting system that incorporates multi-layer authentication, real-time monitoring, and predictive fraud detection, ensuring enhanced security, transparency, and reliability in modern electoral systems.

## 2. Literature Survey

Anagreh et al. [8] proposed an analysis of voter intention to use electronic voting systems by examining factors such as usability, trust, and perceived security. Abu-shanab et al. [9] proposed electronic voting systems as a tool for enabling electronic democracy by facilitating transparent and efficient electoral processes.

Suki et al. [10] proposed a study on decision-making and satisfaction in campus electronic voting systems by analyzing the moderating effect of trust in system adoption. Lin et al. [11] proposed a blockchain-based complete self-tallying electronic voting protocol that enabled secure vote aggregation without requiring a central authority.

Neziri et al. [12] proposed a blockchain-based distributed electronic voting system that ensured anonymity and privacy through cryptographic mechanisms. Mohammadi et al. [13] proposed an analysis of the relationship between democracy and economic growth within sustainable development frameworks. Hamdi et al. [14] proposed an analysis of electronic government systems as a driver for economic growth by improving administrative efficiency and public service delivery.

Shahzad et al. [15] proposed a trustworthy electronic voting system using adjusted blockchain technology to enhance security, transparency, and auditability. Mac Donald [16] proposed an international election observation report that evaluated electoral processes and transparency in Uzbekistan presidential elections. The study assessed compliance with democratic standards and operational practices. Mugnier [17] proposed an overview of the Republic of Uzbekistan focusing on geographical and mapping aspects relevant to governance and infrastructure. The work lacked relevance to electronic voting technologies.

Onur et al. [18] proposed ElectAnon, a blockchain-based anonymous and scalable ranked-choice voting protocol that ensured voter privacy and efficient vote counting. Goloshchapova et al. [19] proposed an analysis of electronic government systems as a key factor for economic prosperity and sustainable development in the post-COVID era.

Gao et al. [20] proposed a blockchain-based solution for notarial services in electronic government systems to ensure secure and verifiable document management. Benabdallah et al. [21] proposed a systematic literature review of blockchain-based electronic voting solutions, analyzing system architectures, security mechanisms, and performance challenges. The study identified key trends and limitations in current approaches.

## 3. Proposed System

Figure 1 illustrates the architecture of a smart electronic voting system built around the ESP32, which acts as the central control unit integrating authentication, communication, and output modules. The system incorporates multiple security layers including ESP32-CAM for facial recognition, fingerprint sensor for biometric verification, and keypad input for PIN-based authentication. A regulated power supply ensures stable operation, while output components such as LCD, buzzer, GSM, and IoT modules provide user interaction, alerts, and remote monitoring. The ESP32 processes all inputs through embedded software, ensuring secure vote casting, real-time data transmission, and tamper-proof election management.

**Step 1: Power Supply Unit**: The regulated power supply provides a stable DC voltage to the ESP32 and all connected modules. This ensures uninterrupted and reliable system operation during the voting process.

**Step 2: Multi-Factor Authentication Inputs**: The system integrates multiple authentication mechanisms including fingerprint sensor, keypad (for PIN entry), and ESP32-CAM for facial recognition. These inputs are verified by the ESP32 to ensure that only authorized voters can cast their votes, thereby preventing fraudulent activities.

**Step 3: Data Processing and Voting Logic**: The ESP32 processes the authentication data and executes the voting algorithm through embedded software. It securely manages voter validation, vote casting, and ensures that each user can vote only once.

**Step 4: LCD Display Interface**: The LCD module displays voting instructions, authentication status, and confirmation messages to the voter. This enhances transparency and provides a user-friendly interface.

**Step 5: Buzzer Alert System**: The buzzer acts as an alert mechanism to notify election officials in case of unauthorized access attempts, system errors, or suspicious activities, ensuring immediate response.

**Step 6: GSM Communication Module**: The GSM module enables real-time communication by sending voting status updates, alerts, or notifications to authorized personnel. It ensures remote monitoring even without internet connectivity.

**Step 7: IoT Connectivity for Cloud Monitoring**: The IoT module (via ESP32 Wi-Fi) transmits voting data securely to a cloud server. This allows real-time monitoring, centralized data storage, and ensures tamper-proof election results.

**Step 8: Secure Voting and Result Management**: After successful authentication, the system allows the voter to cast their vote, which is securely stored and transmitted. The integration of IoT and GSM ensures transparency, reliability, and accuracy in election results.

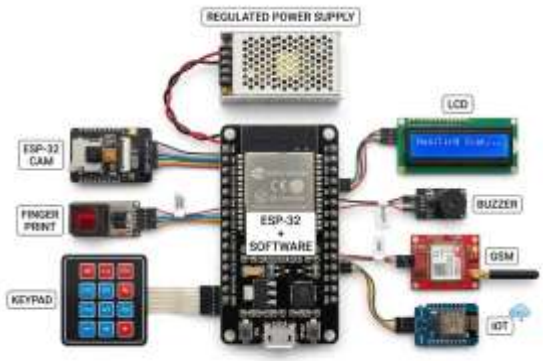



Figure 1. Proposed System

### 3.1 Working Procedure

Figure 2 represents an advanced e-voting system powered by the ESP32 microcontroller, which acts as the central processing unit. The system is powered by a regulated power supply to ensure stable operation. Various input components are connected to ESP32, including an RFID module for voter authentication, polling software for vote management, a keypad for user input, and a fingerprint scanner for biometric verification, enhancing security. The system processes this

data and communicates results through different output modules. The GSM module enables remote communication and notifications, ensuring real-time monitoring. An LCD display provides visual feedback to voters and administrators, while a buzzer acts as an alert system for unauthorized access or errors. Additionally, the IoT module ensures secure data transmission and enables real-time vote tracking and monitoring over the internet. This integration of multiple security and communication components ensures a transparent, efficient, and tamper-proof e-voting system.

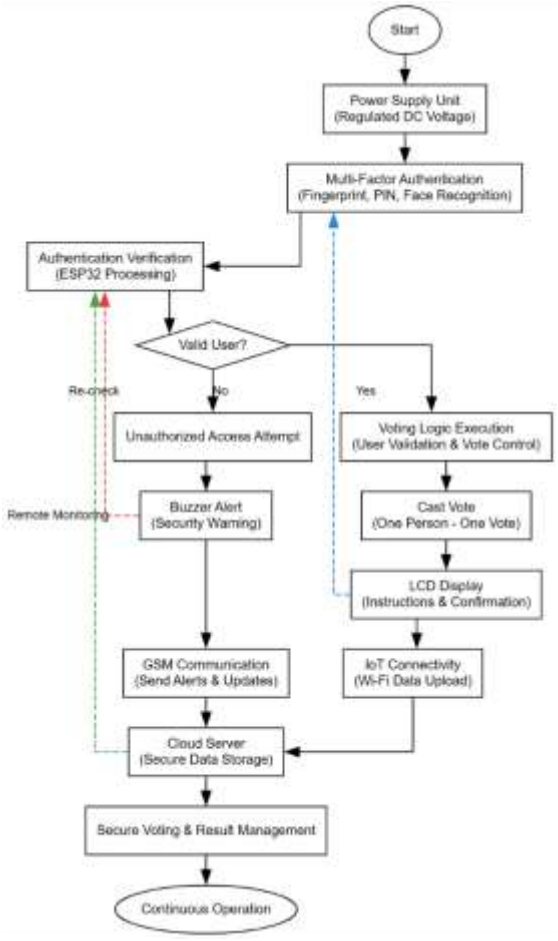



Figure 2. Working Flowchart.

Figure 3 shows illustrate an ESP32-based electronic voting system integrating various input and output components. The ESP32 microcontroller acts as the central unit, handling input and output operations. Below are the pin connections:

**Inputs:**

- **Fingerprint Sensor (FP)**: GPIO2, GPIO4 → Used for biometric authentication.
- **Polling Switches** (User voting input): GPIO5, GPIO18, GPIO19, GPIO21 → Connected to switches for voting selection.
- **RFID Module** (Voter authentication): GPIO22 → Used to read RFID cards.

**Outputs:**

- 16×2 LCD Display (User interface for information display): GPIO15 → Connected to RS, RE, and D4-D7 for data communication.
- **IoT Module** (Remote monitoring): GPIO15 → Enables online data transfer.
- **GSM Module** (Mobile communication for alerts): GPIO26 → Used for sending SMS notifications.
- **Buzzer** (Audio alert for voting confirmation and security alerts): GPIO23 → Controls buzzer activation.

This circuit provides a secure and automated electronic voting system by integrating multiple authentication mechanisms (fingerprint, RFID), user interfaces (LCD), and communication modules (GSM, IoT). The stable 5V power supply ensures reliable operation of all components

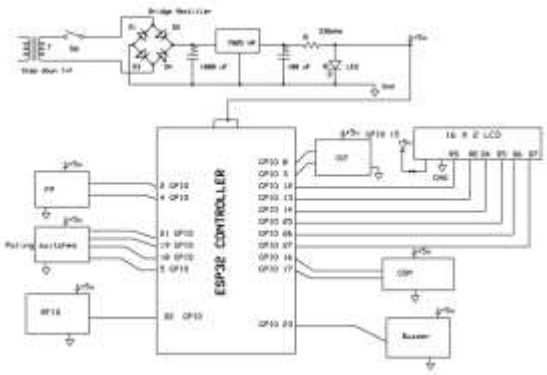



Figure 3. Circuit Diagram.

## 4. Results and Discussion

Figure 4 shows the complete hardware implementation of the IoT-based e-voting system developed using the ESP32 microcontroller. The system integrates biometric fingerprint authentication, keypad voting interface, buzzer alert system, LCD display, and ESP32-CAM for facial recognition to ensure secure and tamper-proof voting.

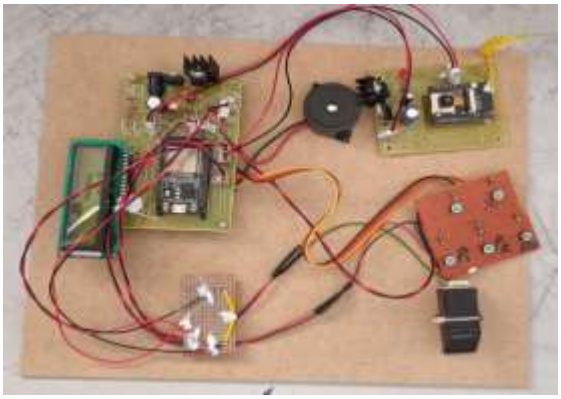


Figure 4. Hardware Prototype of Biometric and CAM Based E-Voting System.

Figure 5 illustrates the LCD interface displaying "Face Recognition – Voting", indicating that the system is verifying the voter through facial authentication. The multi-layer verification process enhances election security and prevents unauthorized voting attempts.




Figure 5. LCD Display Showing Face Recognition Verification.

| S.No | Party1 | Party2 | Party3 | Total | Date |
|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 2026-02-10 14:00:52 |
| 2 | 0 | 1 | 0 | 1 | 2026-01-31 15:44:52 |

Figure 6. IoT Cloud Dashboard Showing Voting Results.

Figure 6 presents the IoT web dashboard used to monitor election results in real time. The interface displays vote counts for different parties along with the total number of votes and timestamps, ensuring transparency and secure monitoring of the voting process.

## 5. Conclusion

The proposed Biometric and CAM-Based E-Voting System presents a secure, transparent, and intelligent solution to modern electoral challenges by integrating multi-factor authentication, real-time monitoring, and IoT connectivity. By combining RFID verification, fingerprint biometrics, and camera-based validation, the system ensures robust voter authentication and significantly reduces the risk of identity fraud and unauthorized access. The inclusion of keypad-based voting and LCD feedback enhances user interaction and accessibility, while GSM-based alerts and buzzer notifications enable immediate detection of suspicious activities. Additionally, IoT integration facilitates centralized monitoring, secure data logging, and real-time result updates, improving transparency and trust in the electoral process. The controlled polling mechanism further ensures proper election management and closure. Finally, this system enhances election integrity, minimizes fraudulent practices, and provides a scalable, efficient, and reliable framework for next-generation digital voting systems.

**References**


[1] Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
[2] Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.
[3] Hamamurad, Q.H.; Jusoh, N.M.; Ujang, U. Factors Affecting Stakeholder Acceptance of a Malaysian Smart City. Smart Cities 2022, 5, 1508–1535.
[4] Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.
[5] Reddy, S. K. R. (2024). Designing Blockchain Architecture to Transform Loyalty Rewards into Cryptocurrency Investments.
[6] Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.
[7] Aljarrah, E.; Elrehail, H.; Aababneh, B. E-Voting in Jordan: Assessing Readiness and Developing a System. Comput. Hum. Behav. 2016, 63, 860–867.
[8] Anagreh, L.F.; Arabia, S.; Abu-shanab, E.A. Voter's Intention to Use Electronic Voting Systems. Int. J. E-Bus. Res. 2017, 13, 67–85.
[9] Abu-shanab, E.; Knight, M.B. E-voting systems: A tool for e-democracy. Manag. Res. Pract. 2010, 2, 264–274.
[10] Suki, N.M.; Suki, N.M. Decision-Making and Satisfaction in Campus e-Voting: Moderating Effect of Trust in the System. J. Enterp. Inf. Manag. 2017, 30, 944–963.
[11] Lin, Y.; Zhang, P. Blockchain-Based Complete Self-Tallying E-Voting Protocol. In Proceedings of the 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Lanzhou, China, 18–21 November 2019; pp. 47–52.
[12] Kalae, U. K. (2020). Developing scalable Power BI dashboards for enhanced data analysis and strategic business decision-making. International Journal of Enhanced Research in Science, Technology & Engineering, 9(3), 8–15.
[13] Mohammadi, H.; Boccia, F.; Tohidi, A. The Relationship between Democracy and Economic Growth in the Path of Sustainable Development. Sustainability 2023, 15, 9607.
[14] Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
[15] Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488.
[16] Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782
[17] Purmani, S. S. R. (2025). Streamlining IT operations and service management with agile frameworks. European Journal of Advances in Engineering and Technology, 12(4), 76–81.
[18] Onur, C.; Yurdakul, A. ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol. Distrib. Ledger Technol. Res. Pract. 2023, 2, 1–25.
[19] Goloshchapova, T.; Yamashev, V.; Skornichenko, N.; Strielkowski, W. E-Government as a Key to the Economic Prosperity and Sustainable Development in the Post-COVID Era. Economies 2023, 11, 112.
[20] Gao, Y.; Pan, Q.; Liu, Y.; Lin, H.; Chen, Y.; Wen, Q. The Notarial Office in E-Government: A Blockchain-Based Solution. IEEE Access 2021, 9, 44411–44425.
[21] Benabdallah, A.; Audras, A.; Coudert, L.; El Madhoun, N.; Badra, M. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. IEEE Access 2022, 10, 70746–70759.