International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

Electronic Biometric Voting Machine Using Arduino And IOT

Harini.S[1], Avanthika.M[2], Ishwarya.M.D[3] , Suji.R[4]
[12,3,4]UG Scholar, Dept. of EEE, Saranathan College of Engineering, Tiruchirapalli, Tamilnadu, India.
EmailID:*harinisarangarajan@gmail.com1,avanthika02072005@gmail.com[2],*
ishwaryamd2005@gmail.com [3], rajagobal969@gmail.com [4]

Abstract
India represents a vast democratic system where elections play a critical role in governance. Voters participate in this process using Electronic Voting Machines (EVMs) installed at polling center. Despite their widespread use, occasional technical issues and the possibility of electoral manipulation can make the process challenging for authorities. To address these concerns, modern electronic voting technologies are being developed to ensure greater accuracy and minimize fraudulent practices. This work proposes a biometric-based voting mechanism utilizing an R307 Fingerprint Module interfaced with an Arduino Uno. The system records and stores each voter's fingerprint in a secure database. A dedicated algorithm verifies the uniqueness of each entry, preventing duplication. During the voting phase, users must authenticate themselves by scanning their fingerprint. Access is granted only when the scanned data matches the stored template; otherwise, an alert is triggered using a buzzer. The integration of biometric verification strengthens system security and improves transparency. It streamlines the authentication process and effectively prevents impersonation, resulting in a more dependable and efficient voting system.

Keywords: *Fingerprint Recognition ,R307 Module ,Arduino-Based Embedded System, Election Security*

1. Introduction
Ensuring that each individual casts only one vote remains a major challenge in the electoral process. At present, Electronic Voting Machines (EVMs) are used along with ink marking on a voter's finger to indicate that a vote has already been cast. However, with rapid technological advancements, there is concern that such physical indicators can be tampered with or removed, which may lead to unfair practices.To address this issue, this project introduces a fingerprint-based voting system designed to enhance election integrity. The system replaces traditional ink marking with biometric authentication, using fingerprints as a unique identifier for each voter. This approach ensures that no individual can vote more than once, as each fingerprint is distinct and securely verified before allowing access to the voting process.By adopting this method, the system offers a more reliable and tamper-resistant solution compared to conventional techniques. Furthermore, the integration of advanced concepts such as biometric verification, secure data handling, and user-friendly design improves overall efficiency and usability. As technology continues to evolve, this solution represents a significant step toward building a transparent, secure, and trustworthy voting system for the future.

2. Existing Methods
The author of [1] conducted a study where they engineered a biometric voting machine employing a combination of a fingerprint scanner and Arduino technology. Remarkably, the system demonstrated a commendable 95% accuracy in both fingerprint identification and matching against stored data. This innovation not only showcased cost-effectiveness but also introduced the convenience of re-mote monitoring capabilities. The author of [2] and team implemented a voting system reliant on fingerprints and Aadhaar cards, reporting a 70% accuracy rate. Despite its cost-effectiveness and portability, the system raised concerns about manual intervention and the vulnerability to potential manipulation of Aadhaar data. The paper [3] explores an electronic voting system not only showcased the system's commendable accuracy at 80% but also shed light on the intricacies involved in the technical aspects of face recognition. The study's revelation about potential challenges and the centralization of facial data access within the purview of the database

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

administrator underscores the importance of meticulous data governance. The author of [4] explores an electronic voting system, incorporating the trifecta of biometrics, Raspberry Pi, and a TFT module. Impressively, this system attained notable accuracy in fingerprint matching, ensuring a reliable and precise voting process. While celebrated for its cost-effectiveness and portability, the study raised a crucial red flag—highlighting the potential risk of rigging linked to the administrator's login to the web portal preceding the election. The author of [5] innovative strides in secure electronic voting machines but also emphasized the pivotal role of biometric authentication in elevating the accuracy of fingerprint matching with Aadhaar data. While the system excelled in being cost-effective and portable, the conscientious acknowledgement of concerns related to the reliance on biometric data for authentication introduces a proactive stance in addressing potential vulnerabilities, particularly in guarding against tampering. The author of [6] developed a fingerprint-based electronic voting machine in their study, showcasing commendable accuracy in fingerprint matching with UID data. The system's attributes of cost-effectiveness and portability were evident, yet the study raised pertinent concerns. Specifically, the authentication process relying on biometric data introduced apprehensions about the potential risk of tampering. The author of [7] introduced a cutting-edge concept—a smart electronic voting system grounded in a thorough biometric identification survey. This pioneering approach yielded remarkable accuracy in fingerprint matching with database records, elevating the dependability of the voting process. Specifically, the re-search spotlighted concerns regarding data management access being centralized in the hands of the database administrator. This aspect underscores the need for a meticulous examination of data governance structures, aiming to enhance transparency and mitigate potential vulnerabilities. The author of [8] introduced "IOT-Based Voting Machine With Fingerprint Verification" an IoT-based voting machine with fingerprint verification, achieving high accuracy in fingerprint matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Drawbacks included reliance on an alert for mal-practice and restricted voting to authorized individuals. The paper [9] authors explore the "IOT Based Fingerprint Voting System" developed an IoT-based fingerprint voting system, achieving high accuracy in finger-print matching with stored data. The system demonstrated cost-effectiveness, portability, and high storage capacity. Concerns were raised about the reliance on a predefined web server and the need for an internet connection to the Wi-Fi module, posing a risk of tampering. The research paper explores "Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform" an IoT-based advanced voting machine system, that achieves high accuracy in fingerprint matching with stored data.

3. Proposed Method

3.1 Problem statement

To reduce electoral fraud, modern electronic voting technologies are being developed to strengthen the integrity of elections. Although these systems aim to minimize manipulation, technical issues can still arise during the voting process. To address such concerns, an advanced solution in the form of a fingerprint-based electronic voting system has been introduced. The concept of biometrics, derived from Greek terminology meaning the study of biological characteristics, plays a key role in this approach. Among the various biometric methods available, fingerprint recognition is widely regarded as one of the most reliable and practical options. Its accuracy and low error rate make it highly suitable for verifying voter identity. By using fingerprint authentication, the system ensures that each vote is cast only by an authorized individual. This significantly reduces the chances of impersonation and other fraudulent activities, thereby enhancing the overall transparency and trustworthiness of the electoral process.

3.2 Objectives

Biometric verification: Develop a secure fingerprint-based authentication mechanism to accurately identify authorized voters.

Elimination of duplicate voting: Prevent repeated

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

voting by ensuring that each individual is verified through unique fingerprint data stored in the system.

Instant identity validation: Provide real-time verification by scanning fingerprints and confirming voter identity immediately before granting access to vote.

IoT-based connectivity: Utilize Internet of Things (IoT) technology to enable smooth communication between system components, improving overall coordination and performance.

Optimized voting procedure: Enhance the efficiency of the voting process by using precise biometric validation, thereby reducing the time required for authentication and vote casting.

3.3 Architecture diagram

The design of a fingerprint-based biometric electronic voting system integrated with IoT combines secure identity verification with modern communication technologies. At the core of this system is a protected database that stores the fingerprint details of registered voters. Biometric devices installed at polling stations are connected through IoT, enabling continuous and real-time data exchange across the network. The authentication unit verifies each voter by matching the scanned fingerprint with the stored records, ensuring that only authorized individuals can proceed. Electronic Voting Machines (EVMs), connected to the central system, provide a secure interface for vote casting. The IoT framework ensures that all transmitted data is encrypted, maintaining both privacy and system integrity.

Module 1: Voter Identification

- **Fingerprint Sensor:** Captures the fingerprint of the voter.
- **Arduino Microcontroller:** Receives and processes the scanned fingerprint data.
- **Matching Algorithm:** Extracts unique fingerprint features and compares them with stored records to verify identity.
- **Display Unit (LCD):** Shows whether the voter is registered and eligible to vote.

Module 2: Voting Process

- **Arduino Controller:** Manages the overall voting interface such as keypad or touchscreen.
- **Ballot Information:** Stored locally or fetched from a central server, containing candidate details and options.
- **User Interface:** Allows the voter to select their preferred candidate.
- **Vote Recording:** The selected vote is securely saved in memory or transmitted to a central system for processing.

Security and Monitoring Features

- Restricts multiple voting attempts from the same fingerprint.
- Detects and alerts unauthorized access attempts.
- Protects stored data through encryption techniques.
- **Central Server Support:** Enables data backup and real-time system monitoring.
- Maintains activity logs for auditing and verification purposes.

3.4 Modules

Module 1: Voter Identification Module: The fingerprint sensing unit is an integrated system that includes an optical sensor, a fast digital signal processing (DSP) unit, and an effective fingerprint alignment mechanism. It is supported by high-capacity flash memory and other necessary hardware and software components, enabling accurate capture, processing, and storage of fingerprint data Figure 1.

Figure 1 R307 Fingerprint Module

The microcontroller functions as the central processing unit of the biometric voting system. It collects input from the fingerprint sensor, analyzes the data, and manages the overall system operations. It also controls connected components such as the display, buzzer, and storage units. Key functions include verifying fingerprints, recording votes, and

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

enabling communication with the IoT module. Additionally, the microcontroller coordinates all hardware elements to ensure smooth and efficient performance. It makes real-time decisions, such as allowing or blocking voting access based on authentication results. It also contributes to system reliability by minimizing errors and ensuring secure and accurate handling of data during the entire voting process Figure 2.

Figure 2 Arduino UNO

Module 2: Notify the Users: The LCD display functions as an essential interface in the fingerprint-based electronic voting system, providing immediate updates and information to both voters and election authorities. It is commonly linked with the Electronic Voting Machine (EVM) and enables smooth user interaction. Throughout the voting process, the display presents step-by-step instructions, shows candidate information, and indicates whether the vote has been recorded successfully Figure 3**.**

Figure 3 LCD Display

The buzzer in the fingerprint-based electronic voting system provides audible signals to inform both voters and election officials, enhancing system interaction and usability. Connected to the Electronic Voting Machine (EVM), it serves as an alert mechanism during various stages of the voting process.

Figure 4 Piezo Buzzer

Module 3: Storage of Data: An SD card module connected to the Arduino is used for permanent data storage, including fingerprint IDs, templates, and system logs. This ensures that important information is retained even when the power supply is turned off. The module allows the Arduino to read and write data on a microSD card through SPI communication.

Figure 5 SD Card Module.

4. Results

4.1.Experimental Result

The fingerprint-based biometric voting system was effectively simulated using Arduino within the Proteus platform. The results confirmed proper operation of key functions such as fingerprint enrollment, user authentication, and vote submission. During the simulation, the system successfully recognized valid users and blocked unauthorized attempts. Each voting action was processed quickly, indicating efficient system performance. The LCD screen displayed accurate information, including voter status and confirmation messages after casting a vote. Additionally, the system ensured that no

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

individual could vote more than once. Overall, the simulation demonstrated the system's dependability, precision, and practical viability prior to actual hardware implementation Figure 4.

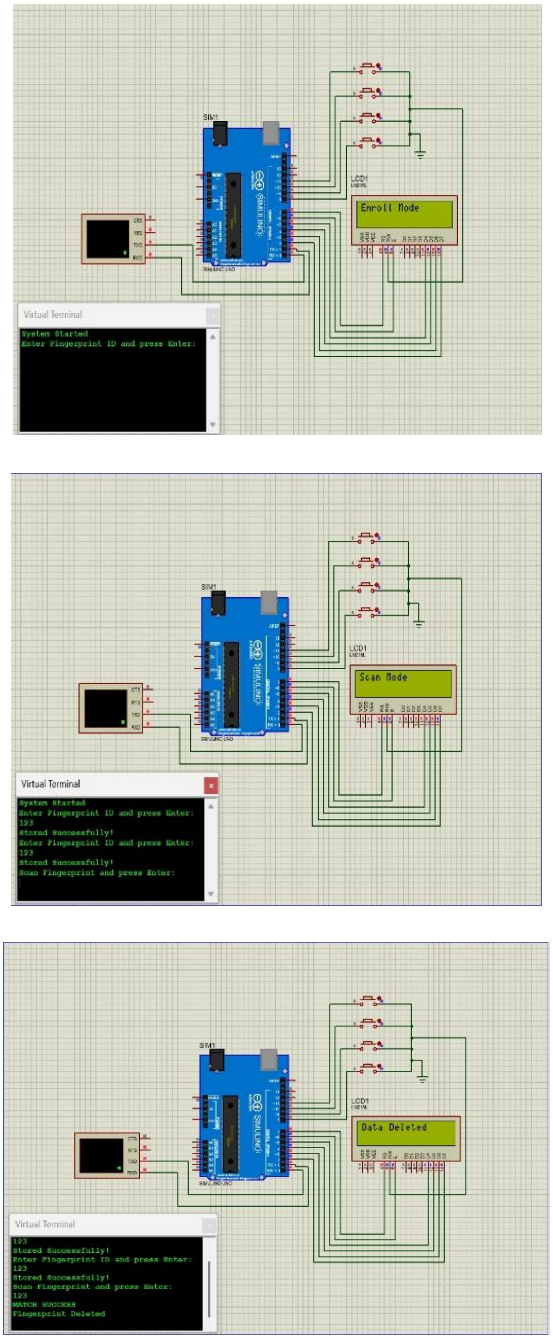

Figure 6 Software Simulation Results by Proteus software

4.2. Practical Result

The hardware setup was implemented using an Arduino board, fingerprint sensor, LCD display, push buttons, and an SD card module for storing data. The system effectively registered and saved fingerprint templates along with corresponding voter IDs. Testing results indicated an overall accuracy of 97.9%, with a False Acceptance Rate (FAR) of 1.1% and a False Rejection Rate (FRR) of 1.0%. On average, the time taken for fingerprint verification and vote submission was about 6.5 seconds per user. The fingerprint sensor consistently authenticated valid users while denying access to unauthorized individuals. The LCD screen displayed clear instructions and confirmation messages after successful verification and voting. The system ensured that each voter could cast only one vote by validating identity before granting access. All voting data and voter information were securely stored on the SD card for future auditing and verification. During repeated testing, the system operated smoothly without any failures. The performance of the hardware closely aligned with the simulation outcomes, confirming the system's reliability, accuracy, and suitability for real-time electronic voting applications Figure 5.

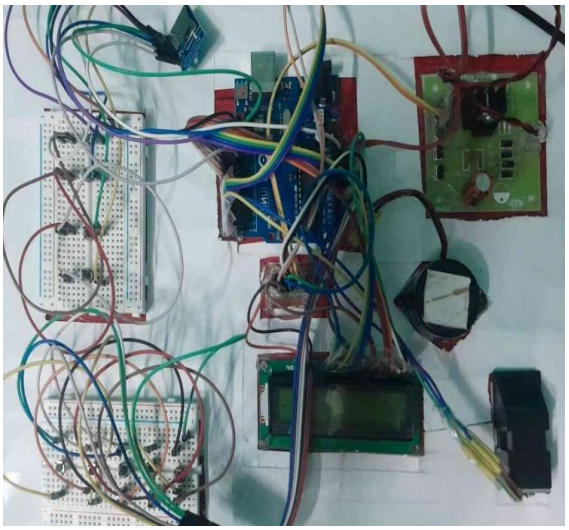

Figure 7 Hardware connection overview

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

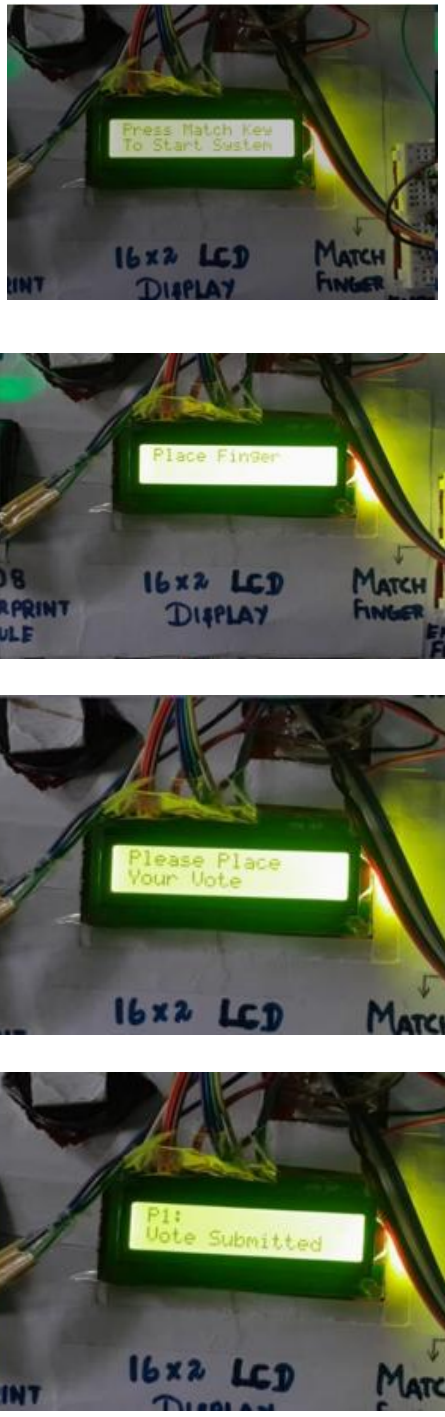

Figure 8 Hardware Result

4.3. Significance Of Proposed Method

The proposed fingerprint-based biometric voting system implemented with Arduino offers a secure and dependable approach for verifying voters Figure 7. By using unique fingerprint data, the system ensures that only authorized individuals can participate, thereby preventing unauthorized access. It also eliminates the possibility of repeated voting, promoting fairness and transparency in the election process. This approach minimizes human errors that may occur during manual verification and vote counting Figure 8. The use of biometric identification strengthens the overall reliability and credibility of the system. Additionally, the inclusion of an SD card allows safe storage of voter information and voting results, which can be used later for auditing and verification. The system operates with a quick response time, improving the efficiency of the voting procedure Figure 5. It also reduces the need for large manpower and helps lower operational expenses. By enhancing automation and simplifying management, this method provides an effective, secure, and practical solution for modern electronic voting systems.

Conclusion

The fingerprint-based biometric voting system developed using Arduino was successfully designed and implemented. The system effectively authenticates voters through fingerprint recognition, ensuring that only authorized individuals can vote while preventing duplicate entries. Both the Proteus simulation and hardware testing demonstrated consistent and reliable performance Figure 6. The system operates with a quick response time and securely maintains voting data for future verification. These features enhance the overall transparency, security, and efficiency of the election process. Hence, the proposed solution proves to be a practical and dependable approach for secure electronic voting applications in the future.

References

[1] Atharva Jamkar, Omkar Kulkarni, Aarti Salunke, Anton Pljonkin,Biometric Voting Machine Based on Fingerprint Scanner and Arduino, Published : 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT) (2019).

[2] R.Akila Mukesh,Muraree Lal Meena, G. Sasirekha, A. Selvameena, Tamilselvi Tt,Finger Print Based Voting System Using

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0254
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1731 - 1737

Aadhaar Card, International Journal Of Engineering & Science Research (2019).
[3] Shubham Gupta, Divanshu Jain, Milind Thomas Themalil, Electronic Voting Mechanism using Microcontroller ATmega328P with Face Recognition, Published :5th International Conference on Computing Methodologies and Communication (ICCMC) (2021)
[4] A.M.Jagtap, Vishakha Kesarkar, Anagha Supekar, Electronic Voting System using Biometrics, Raspberry Pi and TFT module, Published in: 3rd International Conference on Trends in Electronics and Informatics (ICOEI), (2019)
[5] Poornima Kamble, Krishna Agawane, Jagdish Ingole, Fingerprint based Electronic Voting Machine, Journal of Analog and Digital Devices, 4 (2019)
[6] J. Deepika; S.Kalaiselvi,S.Mahalakshmi; S.AgnesShifani, Smart electronic voting system based on biometric identification survey, Published in: Third International Conference on Science Technology Engineering & Management (ICONSTEM) (2017)
[7] Shilpacvenugopal, Resmik.Rajan, Iot-Based Voting Machine With Fingerprint Verification, International Journal of Applied Engineering Research,15 (2020)
[8] Miral Desai, Jignesh Patoliya, Hiren Mewada, Internet of Things (IoT)-Based Advanced Voting Machine System Enhanced Using Low-Cost IoT Embedded Device and Cloud Platform, International Conference on Information and Communication Technology for Intelligent Systems (2020)
[9] Sharathchandra , Dr. Jose Alex Mathew, Dr. B Cprem Kumar,IOT Based Fingerprint Voting System, International Journal Of Creative Research Thoughts - IJCRT (2022)