Gyps Publication

Journal of Computers and Applications, 1(1):41–45, (July-December) 2025. DOI: 10.58613/jca114

Journal of Computers and Applications

Journal homepage: https://www.gpub.org/journal-details.php?journal-id=44

Journal of Computers and Applications

Gyps Publication

Research Article

Secured Digital Voting Machine Using Fingerprint Recognition

Zhang Yong[1]

[1]*School of Mathematics and Physics, Changzhou University, 213164, China.*
[*]*Corresponding author: yzhangczu@aliyun.com*

Article Info

Keywords: *Fingerprint Recognition, Biometric Authentication, Electronic Voting Machine (EVM), Secure Digital Voting, Data Encryption.*

Received: *05.10.2025;*
Accepted: *01.11.2025;*
Published: *15.11.2025*

Abstract

The credibility of any democratic process depends on secure, transparent, and tamper-proof elections. Traditional voting methods, including paper ballots and conventional Electronic Voting Machines (EVMs), remain susceptible to impersonation, multiple voting, unauthorized access, and manual verification errors. To address these limitations, this project proposes a Secured Digital Voting Machine using Fingerprint Recognition, integrating biometric authentication with encrypted electronic voting.

The system employs a fingerprint scanner and biometric module to uniquely verify each voter, ensuring the principle of "one person, one vote" while preventing duplication and impersonation. Once authenticated, the voter interacts with a user-friendly interface to cast their vote, which is securely stored in encrypted digital memory. Additional modules such as secure VPN-based networking, audit trail logging, and data encryption/decryption enhance the system's integrity, confidentiality, and traceability.

Designed with affordable hardware and practical implementation in mind, the proposed system is suitable for institutional and local-level elections, particularly in regions facing challenges like fraud, low digital literacy, and limited infrastructure. This project not only strengthens election security but also provides valuable hands-on exposure to embedded systems, biometric technologies, and digital security concepts. The prototype demonstrates a reliable, efficient, and tamper-resistant solution capable of enhancing trust and transparency in the electoral process.

1. Introduction

Elections are the cornerstone of democracy, providing citizens with the power to choose their representatives and shape the governance of a nation. For an election to be fair and reliable, the voting process must ensure transparency, accuracy, and security while maintaining voter confidentiality. However, traditional voting methods—such as paper ballots and conventional electronic voting machines (EVMs)—continue to face challenges including impersonation, multiple voting, ballot tampering, and unauthorized access. These issues compromise the credibility of elections and reduce public trust in the democratic process.

To overcome these challenges, modern voting systems are increasingly adopting biometric technologies for voter authentication. Among these, fingerprint recognition stands out as one of the most reliable, cost-effective, and user-friendly biometric methods. Each individual's fingerprint is unique, making it a robust tool for ensuring the principle of—one person, one vote. By integrating fingerprint- based authentication into a secured digital voting machine, it becomes possible to prevent electoral fraud, enhance accuracy, and build confidence among voters.

The proposed project, Secured Digital Voting Machine using Fingerprint Recognition, is designed to provide a tamper-proof and efficient voting mechanism. It combines electronic voting with biometric verification to ensure that only authenticated voters can cast their votes, eliminating duplication and impersonation. Furthermore, the system incorporates data encryption and secures storage techniques to protect voter identity and maintain election integrity.

How To Cite: Zhang Yong. Secured Digital Voting Machine Using Fingerprint Recognition. *Journal of Computers and Applications*, 1(1):41–45, 2025. https://doi.org/10.58613/jca114

This project is especially significant in the context of developing nations and local institutional elections, where issues of fraudulent practices, lack of transparency, and limited trust in electoral systems are common. By providing a secure, reliable, and user-friendly solution, the project aims to contribute toward strengthening democratic practices and ensuring fair representation.

2. Relevance

In the modern democratic landscape, ensuring secure, transparent, and reliable elections is a critical challenge. Traditional voting systems, including paper ballots and conventional electronic voting machines (EVMs), are often vulnerable to fraud, impersonation, and unauthorized voting, which can compromise election integrity and public trust.

The proposed project, Secured Digital Voting Machine using Fingerprint Recognition, is highly relevant because it addresses these contemporary challenges by incorporating biometric authentication to uniquely identify voters. This ensures the principle of —one person, one vote‖, prevents multiple voting, and reduces fraudulent activities.

This system is particularly important in areas with large voter populations, limited administrative resources, or low digital literacy, where maintaining accurate and tamper-proof records is difficult. By integrating finger print recognition, secure data storage, and encryption, the project provides a trustworthy, efficient, and user- friendly solution for both institutional and public elections.

From an educational and technological perspective, the project is highly relevant for diploma electrical engineering students, as it combines knowledge of embedded systems, microcontrollers, sensors, and digital security, offering practical experience with real-world applications in modern electronics and information security.

Key Relevance Points:

1. Enhance selection security and transparency.
2. Prevents duplicate voting and impersonation.
3. Builds voter trust in the electoral system.
4. Provides practical exposure to biometric systems and secure electronic design.
5. Aligns with current trends in smart and digital governance systems

3. Literature Review

In recent years, the increasing demand for secure, transparent, and tamper-proof voting systems has prompted researchers to explore biometric technologies— particularly fingerprint recognition—as an enhancement to traditional electronic voting systems.

Siripurapu et al. [1] proposed an enhancement to conventional Electronic Voting Machines (EVMs) by integrating fingerprint and facial recognition technologies. Their system demonstrates improved voter authentication accuracy and a reduction in impersonation threats. The authors emphasize that combining multiple biometric modalities not only strengthens security but also increases system robustness under various environmental conditions.

Olaniyi et al. [2] introduced a secure e-voting system that utilizes fingerprint biometrics in conjunction with cryptographic watermarking to ensure the integrity and confidentiality of votes. Their approach leverages the uniqueness of human fingerprints for voter identification and embeds secure watermarks in vote data to prevent tampering. The study concludes that biometric encryption can significantly improve both authentication and data security in voting systems.

Syed et al. [3] presented a hybrid biometric electronic voting system combining fingerprint and facial recognition for two-factor authentication. Their prototype system aims to minimize election fraud by preventing unauthorized access. They argue that a dual-biometric model provides higher security assurance compared to single-biometric systems, and enhances voter confidence.

Ahmed and Aborizka [4] proposed a secure biometric e-voting scheme focused on privacy preservation. They employed fingerprint recognition along with encryption techniques to ensure that each voter could vote only once while maintaining anonymity. The study highlights the importance of cryptographic protocols in securing not only voter identity but also vote transmission and storage.

Das et al. [5] explored a novel method of fingerprint-based authentication using Human Body Communication (HBC) for remote access. Though not directly focused on voting, the technique demonstrates the potential for secure and efficient biometric authentication in field-deployable systems, with on-device processing enhancing data protection. The relevance to voting systems lies in its promise for low-power, high-security authentication in remote or under-resourced areas.

These studies collectively affirm that integrating fingerprint recognition with electronic voting systems provides a substantial security improvement over conventional EVMs. Moreover, employing cryptographic techniques alongside biometric authentication ensures both voter verification and vote integrity, laying the groundwork for a more secure and transparent democratic process.

4. The Proposed Work

4.1. Problem statement

Free and fair elections are the backbone of any democracy, yet voting systems across the globe still face serious challenges in ensuring transparency, inclusivity, and security.

Fraud and Identity Theft: Conventional Electronic Voting Machines (EVMs) rely heavily on manual voter verification, making them vulnerable to impersonation, duplicate voting, and booth capturing.

Authentication Gaps: Fingerprint-based systems, though more secure, suffer from false rejections (e.g., worn-out fingerprints in elderly/manual workers) and false acceptances due to spoofing attempts using artificial prints.

Cybersecurity Threats: With increasing digitization, risks of hacking, vote manipulation, and data leakage threaten voter privacy and election credibility.

Infrastructure Limitations: In many regions, unstable electricity supply, poor internet connectivity, and limited technical infrastructure hinder smooth operation of advanced voting systems.

Data Privacy & Legal Concerns: Storing and transmitting biometric data raises ethical and legal concerns. Without strong encryption and privacy- preserving measures, sensitive data may be misused.

Public Trust Deficit: Reports of tampering, malfunction, or mismanagement of machines reduce confidence among citizens in the electoral process.

4.2. Objective

1. To design and implement a biometric-based voting system using fingerprint recognition to authenticate voters and ensure —one person, one votell.
2. To prevent electoral fraud, including duplicate voting and impersonation, by verifying the identity of each voter.
3. To provide secure and tamper-proof vote storage using digital encryption and reliable data management techniques.
4. To develop a user-friendly interface suitable for voters of all ages and literacy levels, ensuring accessibility and ease of use.

5. Methodology

5.1. Finger print Scanner

The fingerprint scanner is used to capture and verify the voter's fingerprint in the Secured Digital Voting Machine. It converts the finger impression into a digital template and compares it with pre-stored data to confirm the voter's identity.

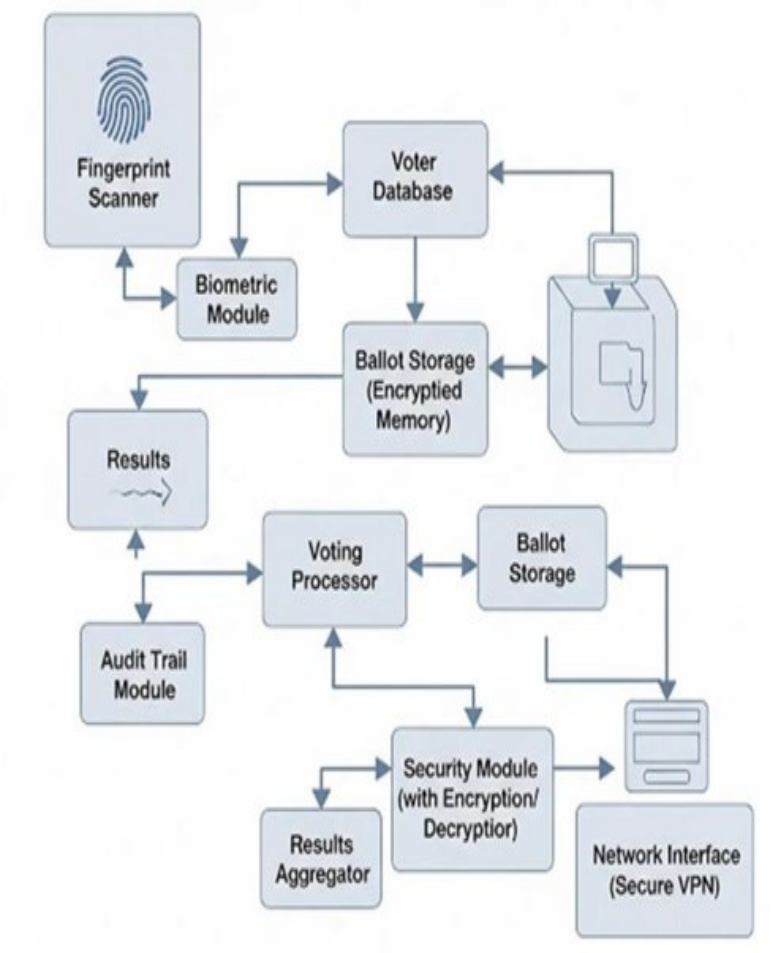

Figure 1: Block diagram of digital voting machine using finger print recognition

Only after successful authentication does the system allow the voter to proceed for casting a vote. This ensures security, prevents duplication, and allows only authorized voters to participate.

5.2. Biometric Module

The biometric module is the core security unit of the Secured Digital Voting Machine using Fingerprint Recognition. It scans the voter's fingerprint, processes it into a digital pattern, and matches it with the stored database. If the fingerprint is valid, it grants access to the voting process; otherwise, it rejects the entry. This ensures that only authorized and unique voters can cast their vote, enhancing the reliability of the system.

5.3. Ballot Storage

The ballot storage in the Secured Digital Voting Machine using Fingerprint Recognition is responsible for securely recording each authenticated vote. Once a voter selects their candidate, the ballot storage saves the voting data in a protected memory unit. It ensures that every vote is stored accurately, without duplication or tampering. At the end of polling, the stored ballots are accessed for result processing and final tally in.

5.4. Security Module (with Encryption/Decryption)

The security module in the Secured Digital Voting Machine using Fingerprint Recognition ensures confidentiality and integrity of voting data. It encrypts the voter's information and ballot records before storing or transmitting them, protecting against unauthorized access. During result processing, the module decrypts the data for accurate tallying. This guarantees a tamper-proof system where all votes remain secure and trustworthy.

5.5. Network Interface (Secure VPN)

The network interface with secure VPN in the Secured Digital Voting Machine using Fingerprint Recognition enables safe communication between voting terminals and the central server. It establishes a private and encrypted channel to transfer voter authentication data and ballot records. The secure VPN prevents hacking, data leakage, and unauthorized access during transmission. This ensures end-to-end protection of election information across the network.

5.6. Audit Trail Module

The audit trail module in the Secured Digital Voting Machine using Fingerprint Recognition maintains a secure logo fall voting activities. It records details such as voter authentication attempts, successful votes, and system events in a tamper- proof manner. This module ensures transparency, accountability, and traceability during the election process. It acts as a reliable backup for verifying results and resolving disputes.

6. Facilities Required

Laboratory Facilities: Access to microcontroller development kits, testing equipment (multimeter, CRO, power supply unit), and soldering/work benches.
Hardware Components: Microcontroller board, fingerprint module, LCD display, keypad, memory unit, power supply, buzzer, and interfacing circuits.
Software Tools: Programming environment for microcontroller (e.g., Arduino IDE, Keil, or Embedded C), simulation software (e.g., Proteus/Multisim) for circuit testing.
Networking Setup: Secure VPN or LAN connection (if network-based communication is implemented).
Support Facilities: Access to a computer lab for coding, database management, and result analysis.
Library and Reference Material: Technical reference books, research papers, and datasheets of components.
Power Backup: UPS/inverter for uninterrupted operation during testing and demonstration.

Table 1: Approx. Expenditure

Sr. No.	Component	Qty.	Approx. Cost (Rs)	Remarks
1	Microcontroller (Arduino Uno/Board)	1	1,500	Main control unit
2	Finger print Module (R305 / R307)	1	3,000	For biometric authentication
3	16×2 LCD Display(with I2C)	1	500	For instructions & results
4	4×4Keypad	1	150	For candidate selection
5	Micro SD Card Module + micro SD Card	1	400	For ballot storage/logs
6	Wi-Fi / Network Interface(ESP8266)	1	300	For secure data transfer (optional)
7	Buzzer/ LED Indicators / Switches	—	200	For alerts & status
8	Power Supply/Battery/ UPS	1 set	800	For reliable operation
9	Enclosure (Cabinet/Box)	1	1,000	To house the system
10	PCB/Breadboard/ Wires/ Connectors	—	500	For circuit assembly
11	Optional Modules (RTC, EEPROM, etc.)	—	500	For added features
TOTAL			**8850 rs**	

Table 2: Time schedule

Month	Work Schedule
Aug 25–Sept 10,2025	Finding problem in searching place (hospital, agriculture, petrol pump, MSEB etc.).
Sept 11–Sept 25, 2025	Discussion on effective problems and identification of most real problem.
Sept 26–Oct 10, 2025	Final selection of problem.
Oct 11 – Oct 25, 2025	Collect references (books, journals, research papers, online sources).
Oct 26–Nov 10,2025	Fixing suitable project title.
Nov 11–Dec 10, 2025	Literature review (study of past work, existing solutions, gap).
Dec 11–Dec 31, 2025	Discussion on costing of project and estimation of budget ($\sim$25k).
Jan 1– Jan 20, 2026	Preparation of block diagram (input–process–output).
Jan 21 –Feb 20, 2026	Methodology and flow chart preparation.
Feb 21–Mar 15, 2026	Draft report preparation (Intro, Problem statement, Literature, Costing, Block diagram, Methodology)
Mar 16–Apr 10, 2026	Correction, editing, and final report writing
Apr 11–Apr 26, 2026	Final submission, viva and presentation.

Article Information

Disclaimer (Artificial Intelligence): The author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.), and text-to-image generators have been used during writing or editing of manuscripts.

Competing Interests: Authors have declared that no competing interests exist.

References

[1] S. L. Rikwith, D. Saiteja, and R. Jayaraman. Enhancement of Electronic Voting Machine Performance Using Fingerprint and Face Recognition. In *Proc. IEEE Int. Conf. on Security, CoLab, 2021*, 2021.

[2] O. M. Olaniyi, T. A. Folorunso, A. Ahmed, and O. Joseph. Design of Secure Electronic Voting System Using Fingerprint Biometrics and Crypto-Watermarking Approach. *J. Inf. Eng. Electron. Bus.*, 8(5):9–17, 2016. MECS Press.

[3] S. N. Syed, A. Z. Shaikh, and S. Naqvi. A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition. arXiv preprint, January 2018.

[4] T. K. Ahmed and M. Aborizka. Secure Biometric E-Voting Scheme, in Proc. In *Int. Conf. on Intelligent Computing and Information Science (ICICIS), Communications in Computer and Information Science, vol. 134, Springer*, pages 380–388. Springer, 2011.

[5] D. Das, S. Maity, B. Chatterjee, and S. Sen. In-field Remote Fingerprint Authentication using Human Body Communication and On-Hub Analytics. arXiv preprint, April 2018.