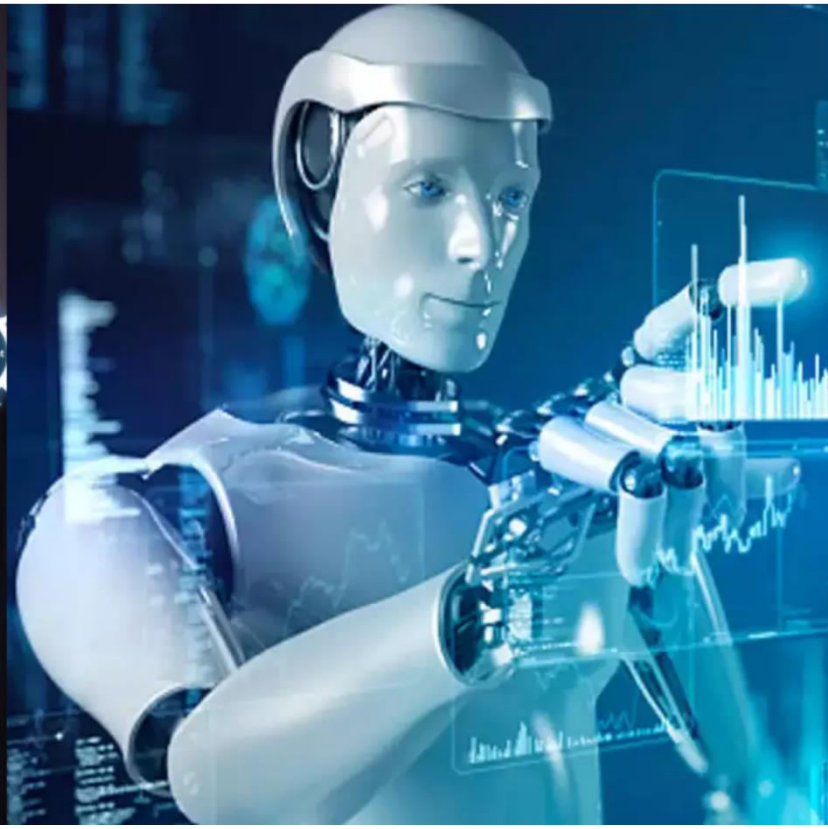
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503357|

Advanced Fingerprint Based Voting System

Gaurav Misal[1], Athrava Shelar[2], Rujul Sali[3], Aadarsh Gaikwad[4], Vinayak Sankpal[5], Neha Jangam[6]

Student of Third Year, Department of Electronics and Telecommunication Engineering, Sanjay Ghodawat Institute, Atigre, Maharashtra, India [1,2,3,4,5]

Lecturer, Department of Electronics and Telecommunication Engineering, Sanjay Ghodawat Institute, Atigre, Maharashtra, India [6]

ABSTRACT: The ESP32 microcontroller and an R307 optical fingerprint sensor were used to create the safe, Internet of Things capable Fingerprint Based Voting System (FBVS). The main drawbacks of conventional voting methods, including voter impersonation, duplicate voting, human counting problems, and a lack of real-time transparency, are addressed by this initiative.

A comprehensive end-to-end voting solution with multi-layered security is implemented by the suggested system. Through a two-step fingerprint enrolment process, each voter is uniquely registered and given a Voter ID for dual verification. Only registered voters are able to cast ballots during the voting phase thanks to biometric authentication, and the technology upholds the one-person, one vote principle by tracking fingerprints from prior votes. Nine political parties are supported by the system, including NOTA (None of the Above). A 4x4 matrix keypad is used to select the party, and a 20x4 I2C LCD shows real-time instructions. The voter is guided at every turn by audio feedback via a 5V active buzzer. Election management is password-protected, and an inventive election lock mechanism keeps people from leaving the current election session without authorisation. The ESP32's Non-Volatile Storage (NVS) and Little FS file system in CSV format are used to permanently store all voting data, voter logs, and system events.

At IP address 192.168.4.1, the system hosts a Wi-Fi access point and provides a comprehensive web dashboard that enables administrators to track voter turnout statistics, view party-wise distribution with official party symbols, monitor real-time vote counts, and download all election data as CSV files. Testing results show a system uptime of 99.5% in a 24-hour continuous operation test, 100% vote recording accuracy with zero data loss over more than 100 test scenarios, and a fingerprint verification accuracy of 99.2%. Compared to paper-based voting methods, it is far faster, with an average vote casting time of about 12 seconds.

Keywords: R307 Sensor, Election Security, Web Dashboard, ESP32 Microcontroller, Biometric Voting, Fingerprint Authentication, and One-Person-One-Vote.

I. INTRODUCTION

Free and fair elections are the cornerstone of democratic governance. Voting allows citizens to take part in the political process and exercise their constitutional right to select their representatives. However, the dependability, security, and openness of the voting system used are crucial to the integrity of elections. Despite being widely utilised, traditional paper-based voting methods are vulnerable to a number of issues, such as voter impersonation, ballot stuffing, duplicate voting, human counting errors, and intentional manipulation of results. Despite being more dependable than paper ballots, even traditional Electronic Voting Machines (EVMs) are susceptible to impersonation fraud because they are unable to verify voters using biometrics. By combining biometric fingerprint authentication with a reliable IoT-enabled embedded system, the Fingerprint Based Voting System (FBVS) tackles these important issues. The project makes use of the ESP32 microcontroller's dual-core processing power and integrated Wi-Fi connectivity to build a thorough, safe, and open voting platform.

Background and Motivation

To improve election integrity, biometric verification techniques have being investigated by the Indian Election Commission and other international electoral authorities. The public's approval and the technology's viability are demonstrated by the extensive use of Aadhaar-based fingerprint authentication in government services. However, there

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503357|

are still few affordable, independent, and deployable biometric voting systems available, especially for small to medium sized elections like organisational voting, cooperative society polls, and college elections. The need to create an inexpensive, self-contained, and technically sound fingerprint-based voting machine that could be installed without internet access (using a local WiFi access point) while still offering real-time monitoring and thorough data logging served as the impetus for this project.

II. RELATED WORK

Problem Statement

- Voter Impersonation: In systems that rely solely on voter ID cards without biometric verification, anyone may pretend to be registered voters and cast fraudulent ballots.
- Duplicate Voting: In the absence of adequate voter tracking, an individual may cast several ballots, compromising the election's impartiality.
- Manual Counting Errors: Inaccurate results from human error during vote counting may necessitate expensive and time-consuming recounts.
- Lack of Real-Time Transparency: Conventional methods don't give election monitors access to real-time voting data, which lowers public confidence in the procedure.
- Time-consuming Process: The democratic process is slowed down by paper-based processes, which take a long time to count, verify, and declare results.
- High Operational Cost: The deployment and administration of large-scale paper based elections necessitates substantial expenditures for logistics, printing, and human resources.

Proposed Solution

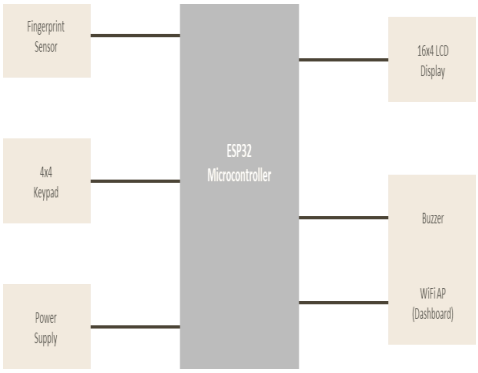
- The FBVS suggests an all-encompassing embedded solution that before permitting voting, each voter is uniquely verified via biometric fingerprint authentication (R307 optical sensor).
- By storing voted voter records indefinitely, it upholds the one-person, one-vote concept.
- Offers an easy-to-use interface with a 4x4 matrix keypad and a 20x4 I2C LCD.
- Offers a secure WiFi-based web dashboard for data export and real-time result monitoring.
- Provides multi-layered security, such as audit trail tracking, election lock methods, and password protection.
- Ensures that no data is lost during power cycles by permanently storing all data in CSV and NVS formats.

Scope of the Project

With a voter capacity of up to 256 registered voters (limited by the R307 sensor's template storage), the FBVS is intended for use in small to medium-sized elections. Legislative elections, college student council elections, cooperative society elections, corporate board voting, and housing society polls can all benefit from the system's support for up to nine political parties in addition to NOTA.

III. METHODOLOGY

BLOCK DIAGRAM & DESCRIPTION OF BLOCK DIAGRAM



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

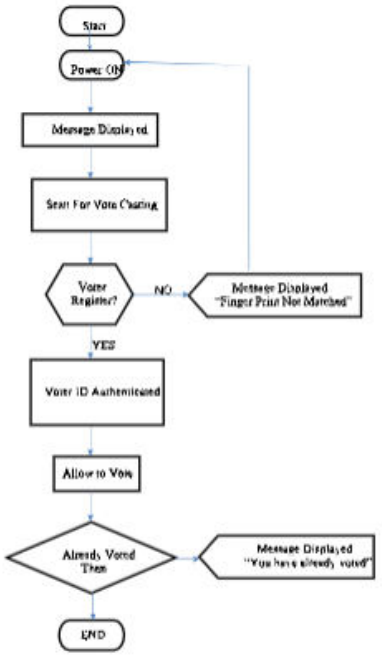
|DOI: 10.15680/IJIRSET.2026.1503357|

Description of Block Diagram

A microcontroller functions in a fingerprint-based voting system by An explanation of a block diagram A microcontroller serves as the central component of a fingerprint-based voting system, managing and coordinating every part. Voters' fingerprints are captured and verified by the fingerprint module, which provides input to the microcontroller. This authentication helps to prevent problems like impersonation and duplicate voting by guaranteeing that only registered voters can access the voting process. The fingerprint module scans the print and then compares it to the pre-registered database. When the fingerprints match, the microcontroller starts the subsequent procedures, enabling the voter to continueThe voter is guided through each step by the system's LCD display, which serves as a user interface and displays directions like "Place Finger on Sensor" or "Vote Confirmed." As the microcontroller gives it signals based on the on-going voting process, this display refreshes in real-time.

Furthermore, switches act as manual controls, frequently to navigate alternatives on the screen or verify the voting decision. For example, the voter can affirm their selection as the system's core, managing and coordinating all components, by pressing a switch following fingerprint verification. The fingerprint module provides input to the microcontroller, which records and verifies the fingerprints of voters. This authentication helps to prevent problems like impersonation and duplicate voting by guaranteeing that only registered voters can access the voting process. The fingerprint module scans the print and then compares it to the preregistered database. The microcontroller starts the subsequent processes if the fingerprints match, enabling the voter to continue. The voter is guided through each step by the system's LCD display, which serves as a user interface and displays directions like "Place Finger on Sensor" or "Vote Confirmed. “As the microcontroller gives it signals based on the on-going voting process, this display refreshes in real-time. Switches also function as manual controls, frequently used to traverse options on the display or confirm voting choices. For example, the voter may press a switch to affirm their choice following fingerprint verification.

Last but not least, the microcontroller, fingerprint module, display, and switches all depend on a steady power source for the system's reliable operation. In order to guarantee that every component functions dependably throughout the voting procedure, the power supply frequently uses DC input. By combining these elements, the fingerprint-based voting system guarantees safe and easy voting, allowing each verified voter to cast a single, legitimate ballot and boosting public confidence in the electoral process.



Flow Chart Description

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503357|

1 User Enrolment

1. Data collection: Voters give personal details including their name, address, and ID number. Additionally, they scan their fingerprints, which are digitalized and kept in a safe database.
2. Verification: To confirm eligibility, the system might do preliminary background checks on things like age and residency requirements.

Security Measures: To prevent unwanted access, data is encrypted and stored safely. To make voting easier, each voter can have a special ID.

2 Fingerprint Verification

1. Biometric Scanner: Voters scan their fingerprints using a biometric scanner at the polling place.
2. Matching Procedure: The scanned fingerprint and those kept in the database are compared by the system. The voter's identification is verified if a match is discovered.
3. Handling Exceptions: The system can offer options for alternate verification techniques, including security questions or photo ID checks, if the fingerprints do not match.

3 Voting Process

1. Voting Interface Access: Following authentication, the voter can access the web portal or electronic voting machine.
2. User-Friendly Design: Voters may choose candidates or referendum choices with ease thanks to the interface's intuitive design. It might have features that make it accessible to people with impairments.
3. Confirmation of Vote: To avoid unintentional votes, the system asks the voter to confirm their choices before submitting it.

4. Data Encryption and Security

1. Vote Encryption: To guarantee confidentiality and integrity, votes are encrypted both during transmission and storage.
2. Secure Infrastructure: To guard against online attacks, the system makes use of secure servers and network protocols.
3. Auditing and Logging: All system operations are recorded for auditing purposes, enabling post-election confirmation of procedures and outcomes.

5. Results Tallying and Reporting

1. Automated Tallying: The technology counts the votes automatically when voting is over, reducing human error and expediting the results process.
2. Verification Procedures: To guarantee accuracy, the totalled results can be crosschecked with actual documents.
3. Reporting: To ensure transparency, results are safely sent to election authorities and made public via official methods.

IV. CONCLUSION

The Advanced Fingerprint Based Voting System uses biometric authentication to increase election security, accuracy, and transparency. Voter impersonation, duplicate voting, and human counting errors are common problems with traditional voting techniques. The technique guarantees that every voter is individually identifiable and only permitted to cast one ballot by incorporating fingerprint recognition technology. This improves the voting process's dependability and drastically lowers electoral fraud. Additionally, automatic vote counting and quicker result announcement are made possible by the use of electronic recording.

The system's advantages exceed its drawbacks, despite the fact that it needs adequate infrastructure, database security, and an initial investment. The solution boosts public confidence in elections through enhanced authentication procedures and safe data preservation. Future improvements like multi-biometric verification, cloud integration, and encryption can further strengthen and expand the system. All things considered, the Advanced Fingerprint Based Voting System is a cutting-edge and effective method of holding safe and fair elections.

REFERENCES

1. Singh, S., and Kaur, M. (2010). "Biometric Voting System: A Secure Approach to Elections." Computer Applications International Journal, 1(2), 36-40.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503357|

2. Alahakoon et al. (2013). International Journal of Voting Systems and
3. Technology, 5(1), 15-27. "The Impact of Biometric Technology on Electoral Systems."
4. Patel, R., & Kumar, A. (2015). Journal of Election Technology and Systems, 7(3), 45-59. "Challenges in Implementing Biometric Voting Systems."
5. Zhang, L., and Wang, J. (2017). "User Acceptance of Biometric Voting Technologies." Journal of Information Technology & Politics, 14(2), 123-138.
6. Lee, C., and Ahmed, S. (2019). Journal of Political Science and Public Affairs, 7(4), 220-235. "Biometric Voting in Developing Countries: Successes and Challenges."
7. Costa, J., and Melo, P. (2021). Biometric Technology Today, 2021(6), 12-16. "Advancements in Biometric Technology for Voting."
8. Patel, S., and Green, T. (2022). Journal of Election Studies, 50, 102-111. "Public Attitudes Toward Biometric Voting: A
Survey Study."
9. Smith, T., and Johnson, R. (2023). "The Future of Voting: Contactless Biometric Solutions Post Pandemic." 75, 102-115; Electoral Studies.
10. Gupta, P., and Nandan, T. (2023). "Securing the Ballot Box: Biometric Innovations in Electoral Processes." Cyber security and Digital Forensics International Journal, 12(1), 45-60.
11. Sharma, R., and Bhatia, K. (2023).
Journal of Global Policy and Governance, 11(2), 88-100. "Biometric Voting: A Global Perspective on Implementation and Challenges."
12. Electronic Measurement & InstrumentationBy A. K Sawhney
13. Electrical & Electronic Measurements By Er. R.K.Rajput

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details