Biometric Based Voter Authentication System

Meera. S[1], Karmugilan. K. V[2], Dhesigan. K. S[3], Ajay. T[4], Logith. A[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Mahendra College of Engineering, Salem.

[2,3,4,5]UG Student, Department of Electronics and Communication Engineering, Mahendra College of Engineering, Salem

DOI: https://dx.doi.org/10.51584/IJRIAS.2026.110400156

Received: 20 April 2026; Accepted: 25 April 2026; Published: 16 May 2026

ABSTRACT

Voting with Fingerprint Technology and the Internet of Things (IoT) will encourage greater confidence in voting due to added security and efficiency during elections. Technology has evolved and traditional voting systems suffer from various issues including impersonation, duplicate voters, and human error when counting or recording the vote. The Fingerprint-Based Voting System using IoT will use fingerprint technology to authenticate votes in order to ensure that only registered voters will be able to vote. Once the voter is verified by the system, that voter can cast his/her vote via push buttons and the system will record the vote at that time. Since data transmissions occur in real-time from IoT Devices to a cloud services provider, the vote can be monitored from anywhere and results will be processed more quickly than under current voting standards. The Fingerprint Based Voting will help avoid multiple voting by changing the status of the voter after they vote. Most importantly, the Fingerprint Voting System will minimize human business and improve voting accuracy, transparency, and reliability for today's digital voting methodologies.

Keywords: Fingerprint Recognition, IoT, Biometric Authentication, Electronic Voting, Cloud Computing.

INTRODUCTION

In a democracy, voting is important, but there are some problems with traditional voting methods (like paper ballots and Electronic Voting Machines - EVMs), including the possibility of fraud, human error, and slow vote count processing .In addition to traditional voting systems, the use of ID cards to validate identity can be abused and allow for unlawful voting. To solve these problems, we have created a system that uses biometric verification with ID cards and the Internet of Things (IoT) to allow for secure, quick and transparent voting. Fingerprints are a proven method for verification since everyone's fingerprint is unique. The IoT allows for devices to communicate with one another in real-time over the Internet. When you combine these technologies, you will have secure voter authentication with fast vote count processing and increased accountability. In addition, this will reduce errors and improve the efficiency of the election process.

LITERATURE REVIEW

Many studies have confirmed that using biometric voting systems will significantly increase the integrity of elections. By utilizing fingerprint sensors and Arduino, researchers have developed a biometric voting application that accurately authenticated voters and reduced fraudulent voting. In addition, researchers created a system using Aadhaar that securely verified a voter's identity and prevented voters from being able to cast a second ballot. Furthermore, the use of facial recognition technology to authenticate voters has created an additional layer of security for the voting process. While these biometric systems have been trying to solve the problem of transparency in elections, most of them do not provide real-time monitoring or are too complex to operate. This proposed system will be a very simple, secure, and efficient method for voting by combining biometric fingerprint authentication with Internet of Things (IoT) technology to allow for seamless, real-time

communication of voter data. Overall, the body of literature indicates the significant value and potential benefit of combining biometric authentication with IoT to create a more secure, trustworthy, and open voting system.

Proposed System

Fingerprint authentication and IoT technology has been proposed for secure voting. Voters register using their fingerprints which are stored in a database (DB). During the voting process, the voter's fingerprint is compared with the stored fingerprint in the DB and only valid fingerprints are granted access to the voting device. Voters cast their votes using push buttons on the voting device and then the vote is sent to the microcontroller for immediate storage and will prevent duplicate votes by updating each voter's status. IoT technology will transmit voting data from the voting device to a cloud server to provide real-time monitoring of the voting process. An LCD display will provide instructions and information to the user throughout the process of voting. This system is user-friendly, secure and appropriate for both small and large elections.

METHODOLOGY

Voter Registration

In the initial stage, each voter's fingerprint is captured using a fingerprint sensor and stored in the system database with a unique voter ID. This registration ensures that only authorized voters are allowed to participate in the election process.

Fingerprint Authentication

During voting, the voter places their finger on the fingerprint sensor. The sensor scans the fingerprint and sends the biometric data to the microcontroller. The system compares the scanned fingerprint with the stored fingerprint data in the database to verify the voter's identity.

Eligibility Verification

After successful fingerprint verification, the system checks whether the voter has already voted. If the voter has not voted previously, the system allows access to the voting interface. If the voter has already voted, the system denies access and displays a message.

Vote Casting Using Buttons

Once the voter is authenticated, the push buttons corresponding to different candidates are activated. The voter selects their preferred candidate by pressing the respective button. Each button represents a specific candidate or option.

Vote Recording

When a button is pressed, the microcontroller records the vote in its internal memory. At the same time, the system updates the voter status to indicate that the voter has already voted, preventing duplicate voting.

IoT Data Transmission

The recorded voting data is transmitted to a cloud server or central database using an IoT communication module such as Wi-Fi (ESP8266 or NodeMCU). This allows election authorities to monitor the voting process and collect results in real time.

Result Monitoring and Storage

All votes are securely stored in the server database. The system enables real-time monitoring, quick vote counting, and accurate result generation after the completion of the voting process.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue IV April 2026

RESULT

The proposed system was tested using different voter inputs, and the authentication responses were recorded and analyzed. The system successfully verified voters based on fingerprint patterns. The results obtained are shown in Table 1.

Voter ID	Authentication Result	Accuracy (%)	Remarks
V101	Success	100%	Valid Voter
V02	Failed	10%	Unauthorized user rejected
V103	Success	100%	Valid Voter
V104	Success	100%	Duplicate vote blocked

The results indicate that the proposed system can accurately authenticate voters using fingerprint recognition. The system effectively identifies valid users and rejects unauthorized or duplicate attempts, ensuring high security. It also operates efficiently in real-time, allowing quick verification and smooth voting. Overall, the system demonstrates high accuracy, reliability, and improved transparency in the voting process.

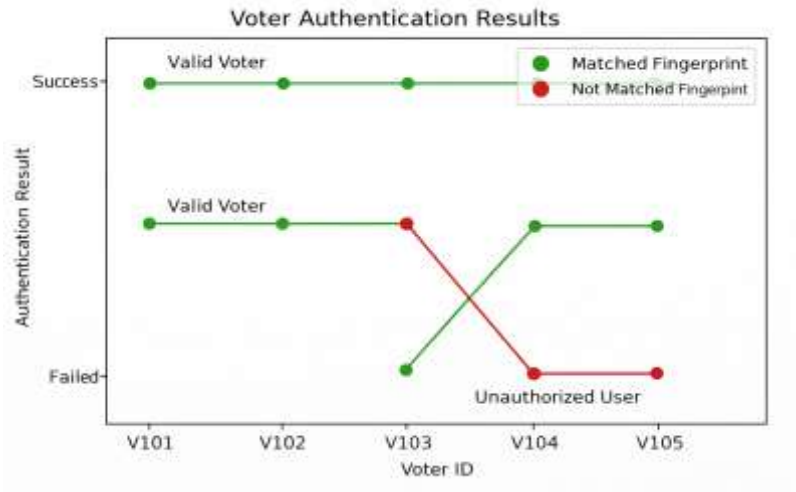

Figure 1: Voter authentication Results

Output

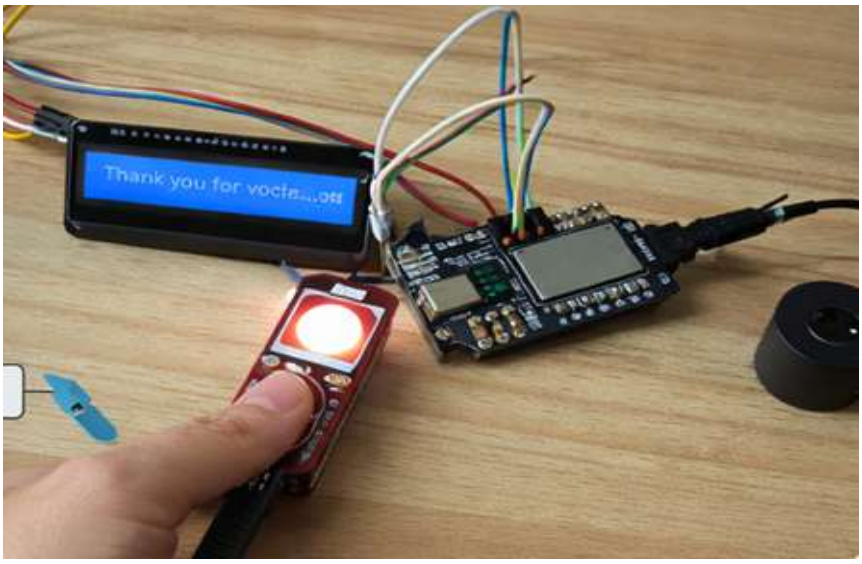

Figure 2: Voter authentication Output Kit

CONCLUSION

An Internet of Things (IoT) Fingerprint Based Voting System provides a secure and practical option to traditional voting methods, eliminating potential for fraud through the use of biometrics for voter authentication, as well as providing transparency due to real time data transmission. In addition, there are reduced errors, time savings, ease of use, and simplification of the voting process. Furthermore, the IoT Fingerprint Based Voting System is designed to be user friendly and scalable to a variety of methods. There will also be future enhancements such as additional multi-factors for authentication to improve security further. Thus, this system will provide fair, accurate and modern elections.

REFERENCES

1. Atharva Jamkar et al., “Biometric Voting Machine Using Fingerprint Scanner and Arduino,” ICCT, 2019.
2. R. Akila Mukesh et al., “Fingerprint-Based Voting System Using Aadhaar Card,” IJESR, 2019.
3. Shubham Gupta et al., “Electronic Voting System Using Face Recognition,” ICCMC, 2021.
4. A.M. Jagtap et al., “Biometric Voting System Using Raspberry Pi,” ICOEI, 2019.
5. Poornima Kamble et al., “Fingerprint-Based Electronic Voting Machine,” Journal of Analog and Digital Devices, 2019.