INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 5, May 2026 | ISSN: 2456-4184 | IJNRD.ORG

ADHAAR UIDAI BASED BIOMETRIC ELECTRONIC VOTING SYSTEM TO PREVENT ELECTORAL FRAUD

[1] Rahul Negi, [2]Arjun Kumar, [3] Poonam Kumari Mahato

[1]Assitant Professor [2]Student, [3]Student,
Electronics and communication Engineering Department,
Tula's Institute, Dehradun, India

Abstract : This paper proposes a biometric-based electronic voting system aimed at improving the security, accuracy, and efficiency of the voting process. Traditional voting methods often face challenges such as voter impersonation, duplication, and manual errors. To overcome these issues, the proposed system uses fingerprint recognition as a reliable method of voter authentication. Each voter's biometric data is registered and stored securely, and verification is performed before allowing access to the voting interface.

The system integrates a fingerprint sensor with a microcontroller and a database to manage voter information and record votes accurately. It ensures that each individual can vote only once, thereby maintaining fairness in elections. In addition, the system reduces the need for manual supervision and enables faster vote counting, improving overall efficiency.

By combining biometric technology with electronic voting, the proposed model enhances transparency and trust in the electoral process. It provides a practical and secure solution that can be adapted for large-scale implementation with further improvements in data security and system scalability.

***Keywords*– Biometric voting, Fingerprint, E-voting, Authentication, security, Encryption, Microcontroller, Verification**

1. INTRODUCTION

A fair and secure voting system is essential for the proper functioning of any democratic society. Traditional voting methods, such as paper ballots and conventional electronic voting machines, often face challenges including voter impersonation, duplicate voting, and human errors during vote counting. These limitations can effect the transparency and credibility of the electoral process, creating a need for more advanced and reliable solutions.

With the rapid development of technology, biometric systems have emerged as an effective way to verify individual identity. Among various biometric techniques, fingerprint recognition is widely used due to its uniqueness, accuracy, and ease of implementation. By integrating biometric authentication into electronic voting systems, it becomes possible to ensure that only eligible voters can cast their votes, thereby reducing the chances of fraud and unauthorized access.

The biometric-based electronic voting machine system combines hardware components such as fingerprint sensors and microcontrollers with software for data processing and secure storage. In this system, each voter's fingerprint is registered in a database and verified at the time of voting. Once authenticated, the voter is allowed to cast their vote, which is securely recorded. This approach not only enhances security but also speeds up the voting and counting process.

The aim of this research is to design and analyze a secure, efficient, and user-friendly voting system that improves election integrity. By reducing manual intervention and incorporating reliable authentication methods, the proposed system contributes to building trust in modern electoral processes.

2. LITERATURE REVIEW

The voting system has undergone significant changes over time to improve reliability and efficiency. The commonly used methods are:

2.1. Paper Ballot System

2.2. Electronic Voting System

2.1. PAPER BALLOT SYSTEM

The paper ballot system was the traditional method used for conducting elections. In this system, voters cast their votes by marking their choice on a ballot paper and placing it in a ballot box. Although this method was simple, it had several limitations.

The process of counting votes was slow and required significant manual effort. Ballot papers were also prone to physical damage due to environmental conditions such as moisture, heat, or mishandling. In some cases, ballots could be lost or destroyed, leading to data loss.

Additionally, this system was vulnerable to fraudulent practices such as fake voting and ballot stuffing. Maintaining and storing large numbers of ballot papers also increased the cost and complexity of elections.

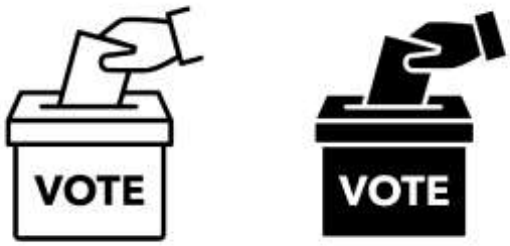

FIG.2.1-BALLOT BOX

2.2. ELECTRONIC VOTING SYSTEM

Electronic Voting Machines (EVMs) were introduced to overcome the drawbacks of paper-based voting. These systems simplified the voting process and reduced the time required for vote counting. EVMs consist of control and balloting units that help record votes electronically.

Despite these improvements, EVMs still face several challenges. One major issue is the lack of strong voter authentication, which can allow unauthorized individuals to vote. There are also concerns regarding systems security, as tampering with the device or its software could affect the results.

Other issues include the possibility of duplicate voting, limited transparency, and difficulty in independently verifying the results. These limitations highlight the need for a more secure and reliable system.

FIG.2.2-EVM System

3. PROPOSED METHOD

The proposed system is a biometric-based electronic voting system that uses fingerprint recognition to provide secure and reliable voting. Instead of using any government databases, a locally created sample database of registered voters is maintained. Each voter's details, including a unique ID and fingerprint, are stored during the enrollment phase.

During voting, the voter places their finger on the fingerprint sensors. The system compares the scanned fingerprint with the stored data in the database. If the voter is verified and has not voted earlier, they are allowed to cast their vote using push buttons. If verification fails or the voter has already voted, access is denied.

A microcontroller (such as Arduino) controls the entire process, including authentication, vote recording, and display of messages on the LCD screen. The system also includes a GSM module, which is used to send notification such as confirmation messages to voters or alerts to the administrator after voting is completed.

Votes are stored securely in the system memory for result calculation. This method ensures one-person-one-vote, reduces fraudulent and transparency of the voting process.

4. EXPERIMENTAL SETUP

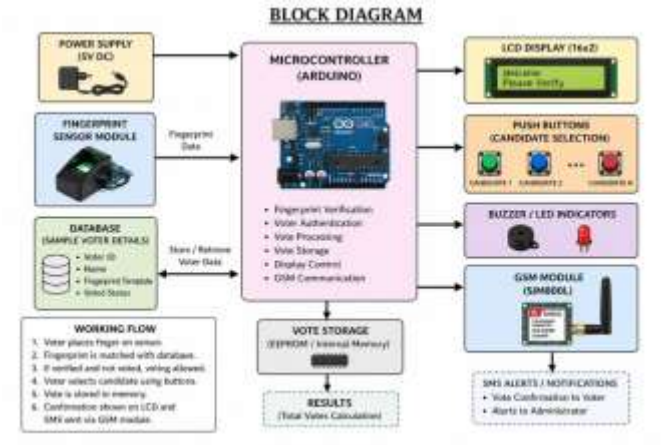

FIG.4.1-BLOCK DIAGRAM

The above figure consist of a microcontroller, fingerprint sensor, database, GSM module, LCD display, push buttons, and power supply. The power supply provides the required voltage to all components.

The fingerprint sensor captures the voter's fingerprint and sends it to the microcontroller. The microcontroller compares it with the stored data in the local database to verify the voter. If the verification is successful, the voter is allowed to select a candidate using push buttons.

The LCD display shows instructions and confirmation messages during the process. Once the vote is cast, it is stored in the system memory. The GSM module sends a confirmation message or alert after voting. LED indicates or a buzzer provide additional feedback.

5. WORKING

Our system has three phases:

- Enrollment
- Voting process
- Result phase

FIG.5.1-Flow chart

PHASE I: ENROLLMENT
In this phase, voter information and fingerprint data are collected and securely stored in the database to create a unique identity for each voter.

PHASE II: VOTING PROCESS
In this phase, the voter is authenticated using fingerprint verification, after which the verified voter is allowed to cast their vote, which is recorded securely in the system.

PHASE III: RESULT PHASE
In this phase, all recorded votes are processed and counted to generate and display the final results accurately.

6. HARDWARE IMPLEMENTATION AND RESULTS

6.1 Experimental results:

The proposed biometric-based electronic voting system was successfully tested using a sample database of registered users. The system was able to perform voter authentication accurately using the R307S fingerprint sensor, ensuring that only authorized users were allowed to access the voting interface.

During testing, the fingerprint module correctly identified valid users and rejected unregistered or duplicate voters, which helped in preventing unauthorized voting. After successful verification, voters were able to select their preferred candidate using the push buttons, and the votes were stored accurately in the system memory.

The 16×2 LCD display provided clear instructions and displayed real-time messages such as voter verification status and vote confirmation, making the system user-friendly. The SIM900A GSM module successfully sent confirmation messages after each vote, improving system transparency and communication.

The buzzer and LED indicators also functioned properly by giving instant audio and visual feedback during the voting process. The overall performance of the system was stable, accurate, and efficient, demonstrating that the proposed method is reliable for secure small-scale electronic voting applications.

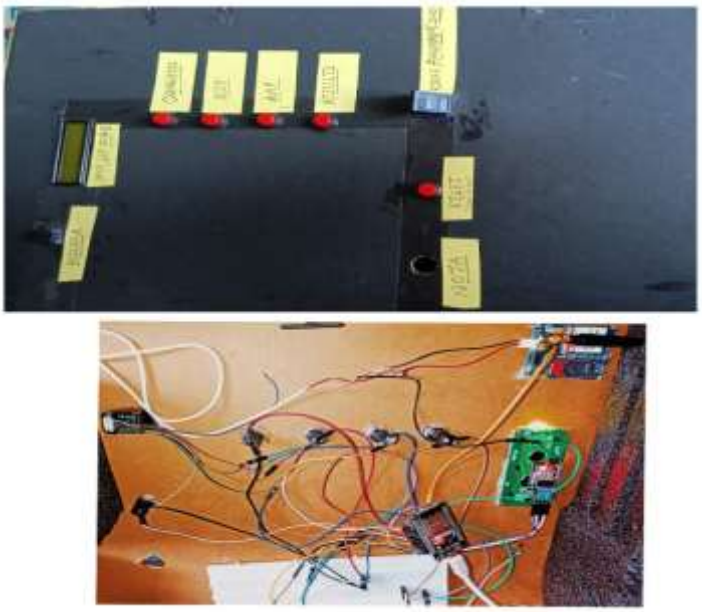

FIG.6.1 Hardware

6.1.1 Enrollment:

The enrollment phase was successfully completed by registering sample voters into the system. During this process, each voter's fingerprint and unique identification details were captured and stored accurately in the local database. The fingerprint sensor performed reliable enrollment, ensuring that every registered voter had a unique record for secure authentication during voting.

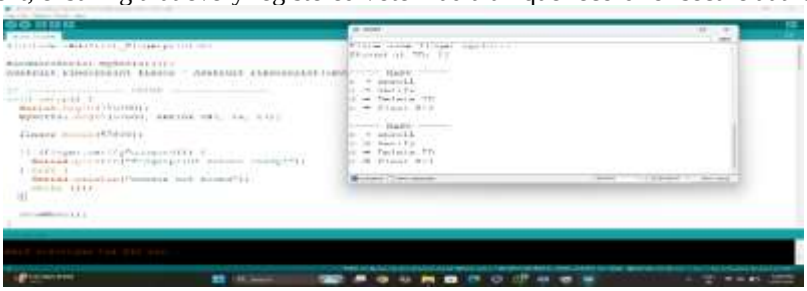

FIG.6.2 Enrollment results

6.1.2 Matching with database:

During the authentication process, the scanned fingerprint of the voter is compared with the fingerprint records stored in the local database. The system successfully matches valid fingerprints and identifies authorized users accurately. If a match is found, the voter is allowed to proceed for voting; otherwise, access is denied. This matching process ensures secure voter verification and prevents unauthorized or duplicate voting.

FIG.6.3 Matching results

6.1.3 Result:

After successful fingerprint authentication and candidate selection, the system records the vote securely in its memory. The LCD display then shows the name of the selected party along with a confirmation message indicating "Voted Successfully", followed by "Thank You". This confirms that the voting process has been completed successfully, and the voter's status is updated in the database to prevent multiple voting, ensuring a secure and transparent election process.

FIG 6.4 Final result

7. CONCLUSION

This project presents a biometric-based electronic voting system designed to improve the security, accuracy, and reliability of the voting process. By using fingerprint authentication, the system ensures that only authorized voters can cast their votes, which helps in preventing duplicate and unauthorized voting.

The use of a locally maintained voter database makes the system suitable for small-scale applications without depending on external government databases. The integration of the GSM module enhances communication by sending vote confirmation messages, while the LCD display provides clear instructions and feedback to the user throughout the process.

The experimental results show that the system performs effectively and records votes accurately. Overall, the proposed system provides a simple, secure, and efficient solution for electronic voting and has the potential for future improvements and larger-scale implementation.

8. FUTURE SCOPE

The proposed biometric-based electronic voting system can be improved further in the future to make it more advanced and useful for large-scale voting applications. Currently, the system uses a sample local database, but in the future it can be connected to a larger database to manage more voters efficiently.

Additional biometric features such as face recognition or iris scanning can be added to increase security and improve voter authentication. Advanced security methods can also be used to protect voter data and make the system safer from unauthorized access.

The system can also be connected to cloud technology and IoT, which will help in storing data securely and accessing voting information from different locations. A mobile or web application can be developed for easier monitoring and management of voting records and results.

With these future improvements, the system can become more secure, reliable, and suitable for use in schools, colleges, organizations, and even large public elections.

9. REFERENCES

[1] K. Ashok and R. Sharma, "Design and Development of Biometric Based Electronic Voting System," International Journal of Engineering Research and Technology (IJERT), vol. 8, no. 6, pp. 245–249, 2020.

[2] P. Kumar and S. Verma, "Fingerprint Authentication for Secure Electronic Voting Machine," International Journal of Computer Applications, vol. 177, no. 12, pp. 15–20, 2019.

[3] A. Gupta and M. Singh, "Implementation of Biometric Voting System Using Arduino," International Research Journal of Engineering and Technology (IRJET), vol. 7, no. 4, pp. 3250–3254, 2021.

[4] R. Patel and N. Mehta, "Smart Voting System Using Biometric Technology," International Journal of Advanced Research in Engineering and Technology, vol. 6, no. 3, pp. 112–118, 2020.

[5] S. Jain and V. Tiwari, "Secure Electronic Voting Using Fingerprint Verification," Journal of Emerging Technologies and Innovative Research, vol. 8, no. 5, pp. 540–545, 2021.

[6] Arduino Official Website

[7] Espressif (ESP32 Documentation)

[8] Adafruit (Fingerprint Sensor Documentation)

[9] SIMCom (SIM900A GSM Module)

[10] LCD Module Basics (16x2 Display) - SparkFun