



Fingerprint-Based Secure E-Voting System Using Biometrics

¹Shilpa N S, ²Dakshatha N, ³Deekshitha H S, ⁴Manasa N

¹Assistant Professor, ²Student, ³Student, ⁴Student

Department of Information Science,
T John Institute of Technology, Bengaluru, India

Abstract:

Electronic voting (e-voting) systems are designed to make elections faster, more efficient, and more transparent compared to traditional paper-based voting. However, many existing systems still face problems like voter impersonation, multiple voting, and tampering with voting data. To solve these issues, this research proposes a secure e-voting system that uses **fingerprint-based biometric authentication**. In this system, each voter's fingerprint is captured and converted into a unique encrypted template, preventing duplication or forgery. When a voter comes to vote, their fingerprint is matched with the stored record to ensure that only the right person can vote—and only once. To protect the security of the votes, encryption methods such as **AES or RSA** are used during both data transmission and storage. The system also generates a unique transaction ID as a receipt for each voter. This allows the voter to confirm that their vote was recorded, without revealing who they voted for. Overall, the proposed system increases transparency, blocks fraudulent activities, and provides strong end-to-end security throughout the election process. Experimental results show that combining biometric authentication with encryption greatly improves the accuracy of voter verification and the overall reliability of the system compared to traditional e-voting methods.

Key Terms: Biometric authentication, Cryptography, Electronic voting (E-voting), Fingerprint recognition, Security, Vote verification, Data encryption.

Introduction:

Electronic voting (e-voting) has become a modern alternative to traditional paper-based voting, offering faster, more efficient, and cost-effective elections. Despite these benefits, many e-voting systems still face serious challenges related to security, voter verification, and data protection. Problems like voter impersonation, multiple voting, vote tampering, and unauthorized system access create doubts about election fairness and reduce public trust.

Biometric authentication provides a strong solution to these issues because it uses unique human characteristics to verify a voter's identity. Among different biometric methods—such as face recognition, iris scanning, or voice recognition—fingerprint identification is one of the most accurate and practical. Fingerprints are unique to every individual and remain the same throughout life, making them ideal for secure voter verification.

A fingerprint-based e-voting system adds biometric checks to the voting process so that only registered voters can vote and each person can vote only once. This improves transparency, removes the need for manual checking, and greatly reduces the chances of fraud. When combined with cryptographic techniques, the system also ensures that votes stay confidential and cannot be altered at any stage.

This research focuses on creating a secure fingerprint-based e-voting system that ensures voter authenticity, data security, and overall election integrity. By combining biometric verification with strong encryption, the proposed system offers a reliable, user-friendly, and transparent voting platform. Through the use of biometric technology, this approach aims to overcome the weaknesses of current e-voting systems and support the development of a safer and more trustworthy election process.

Literature review:

Electronic voting (e-voting) has become an important research area because it offers faster, more transparent, and more accurate elections compared to traditional paper-based methods. Traditional voting systems often suffer from problems like manipulation, slow logistics, and counting mistakes, which has encouraged the shift toward secure digital voting systems. However, e-voting also introduces new risks, including unauthorized system access, voter impersonation, and tampering with stored or transmitted data. To overcome these challenges, biometric authentication has emerged as a more dependable way to verify voter identity.

Biometric authentication uses unique human features—such as fingerprints, iris patterns, and facial characteristics—to identify individuals. Among these options, fingerprint recognition is the most widely adopted because it is accurate, affordable, and easy to integrate with existing hardware. Fingerprints do not change over a person's lifetime and are extremely difficult to forge, making them ideal for secure voting systems. Research shows that fingerprint-based authentication greatly reduces impersonation and duplicate voting, ensuring that only legitimate voters take part in elections.

Many researchers have proposed fingerprint-based e-voting models that incorporate different security techniques. For example, in one study, fingerprint authentication was combined with the AES encryption algorithm to secure both voter data and ballots during transmission. Another system used RSA encryption to ensure that votes stay confidential and cannot be altered after submission. Some researchers have also integrated blockchain technology with biometric systems to create permanent, tamper-proof voting records that improve transparency and trust.

Recent studies have aimed at improving the efficiency and accuracy of fingerprint recognition in e-voting systems. One approach used a minutiae-based matching algorithm to reduce false acceptance and rejection rates. Another study enhanced fingerprint image preprocessing by adding noise removal and advanced feature extraction techniques, resulting in faster and more reliable voter authentication during real-time voting. These developments have made biometric e-voting systems more practical for use in large-scale elections.

Despite these improvements, several challenges still remain. One major issue is the security of stored biometric templates—if attackers access these databases, voter privacy could be compromised. Researchers have suggested solutions such as cancellable biometrics and encrypted templates to protect biometric data from misuse. Another concern is the lack of transparent auditing mechanisms, which can reduce public trust in electronic election results. To address this, recent studies recommend combining biometrics with blockchain to create decentralized, verifiable voting systems that maintain both voter anonymity and system integrity.

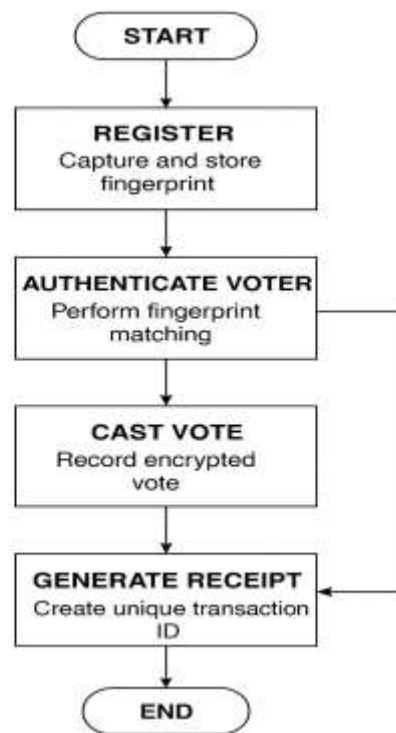
Methodology:

Fig.1.Flowchart

Start

The process begins when a voter accesses the e-voting system to participate in the election.

Registration

During registration, the voter's fingerprint is scanned and converted into a unique encrypted template. This fingerprint data is securely stored in the voter database, ensuring that only genuine and authorized voters are registered.

Authentication

When the voter comes to vote, the system scans their fingerprint again and matches it with the stored template.

- If the fingerprint matches, the voter is allowed to continue.
- If it fails, the voter must re-authenticate.

This step prevents impersonation, duplicate voting, and unauthorized access.

Vote Casting

After successful authentication, the voter proceeds to cast their vote. The selected vote is encrypted using secure cryptographic methods and stored safely in the system to protect confidentiality and prevent tampering.

Receipt Generation

Once the vote is submitted, the system generates a unique transaction ID for the voter. This receipt confirms that the vote was recorded while keeping vote choices secret.

End

The session ends, completing a smooth, secure, and transparent voting process.

Data and Source of Data:

The data used in this fingerprint-based secure e-voting system consists of biometric fingerprint images, basic voter identification details, and system-generated voting session records such as authentication logs, encrypted votes, and transaction IDs. Biometric data is essential for accurate voter verification, while minimal voter

information ensures unique identification without affecting vote privacy. To avoid privacy concerns and ensure ethical research, the system uses publicly available fingerprint datasets such as the FVC (Fingerprint Verification Competition) datasets, NIST Special Database 14, the SOCOFing dataset, and synthetic fingerprints generated through SFinGe. These datasets provide diverse and realistic fingerprint patterns that are widely used in academic research, enabling reliable testing of biometric authentication and overall system performance.

Implementation:

The fingerprint-based secure e-voting system was implemented using four key modules: registration, authentication, vote casting, and receipt generation. During registration, the voter's fingerprint is scanned, converted into an encrypted template, and securely stored with minimal voter details. In the authentication phase, the system matches the live fingerprint with the stored template to ensure only the right voter can access the system. After successful authentication, the voter casts their vote, which is immediately encrypted and saved securely to prevent tampering. Once the vote is recorded, the system generates a unique transaction ID as a receipt to confirm successful voting without revealing the vote. Overall, the implementation ensures a secure, private, and user friendly voting experience.

Setup Environment :

The system was developed using Android Studio with Java/Kotlin and tested on a Windows 10/11 PC. A secure database such as SQLite or Firebase was used to store encrypted fingerprint templates and vote data. A compatible fingerprint scanner (e.g., SecuGen or DigitalPersona) was connected to an Android device running Android 9.0 or above. Basic network connectivity was required for syncing encrypted votes. This setup provided a simple but effective environment to build and test the fingerprint-based e-voting system.

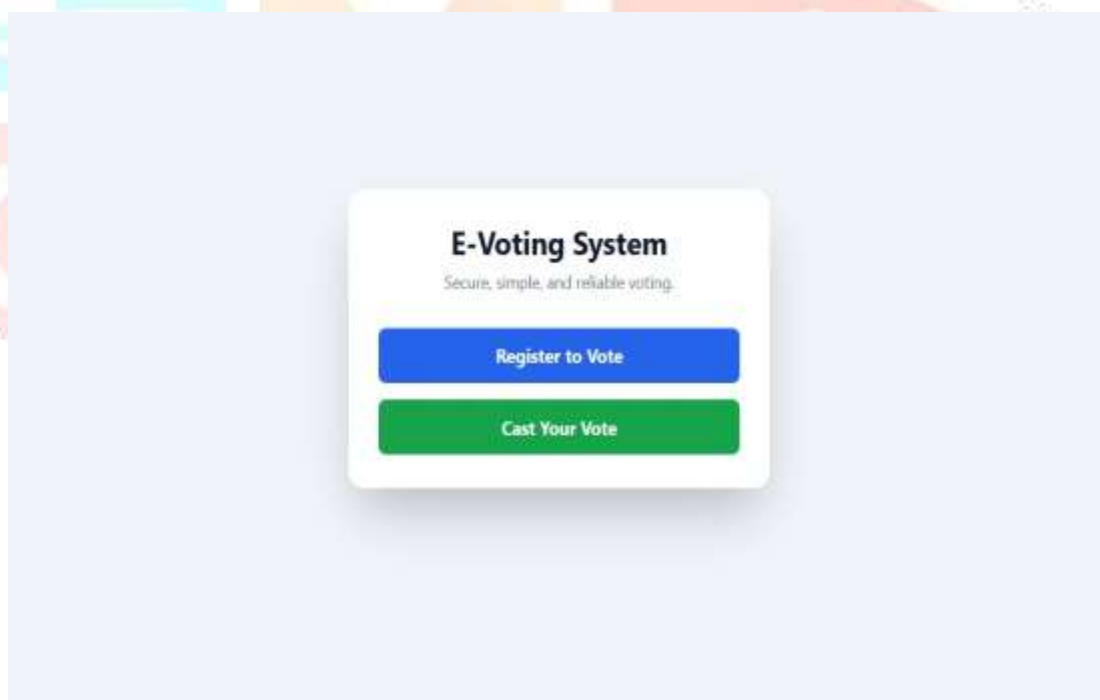
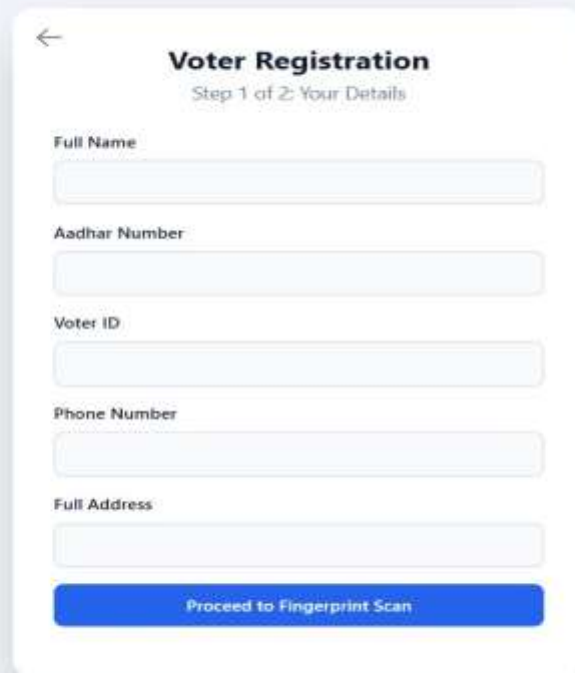


Fig.2.Home Page



A mobile application screen titled "Voter Registration" with a subtitle "Step 1 of 2: Your Details". It features a back arrow in the top left corner. The form contains five input fields: "Full Name", "Aadhar Number", "Voter ID", "Phone Number", and "Full Address". At the bottom, there is a blue button labeled "Proceed to Fingerprint Scan".

Fig.3.Registration Page



Fig.4. Biometric Authentication

RESULTS:

The implementation of the fingerprint-based secure e-voting system produced promising results. The fingerprint authentication module successfully verified registered voters with high accuracy, showing reliable matching even under different lighting and finger-placement conditions. Unauthorized users and mismatched fingerprints were consistently rejected, proving the system's effectiveness in preventing impersonation and multiple voting attempts.

During testing, all encrypted votes were stored securely without any data loss or tampering. The system also generated a unique transaction ID for each voter, allowing them to confirm their participation without revealing their vote. The voting process remained smooth and user-friendly, with quick authentication and fast response times. Overall, the results demonstrate that integrating biometric authentication with encryption significantly improves the security, privacy, and trustworthiness of an e-voting system.

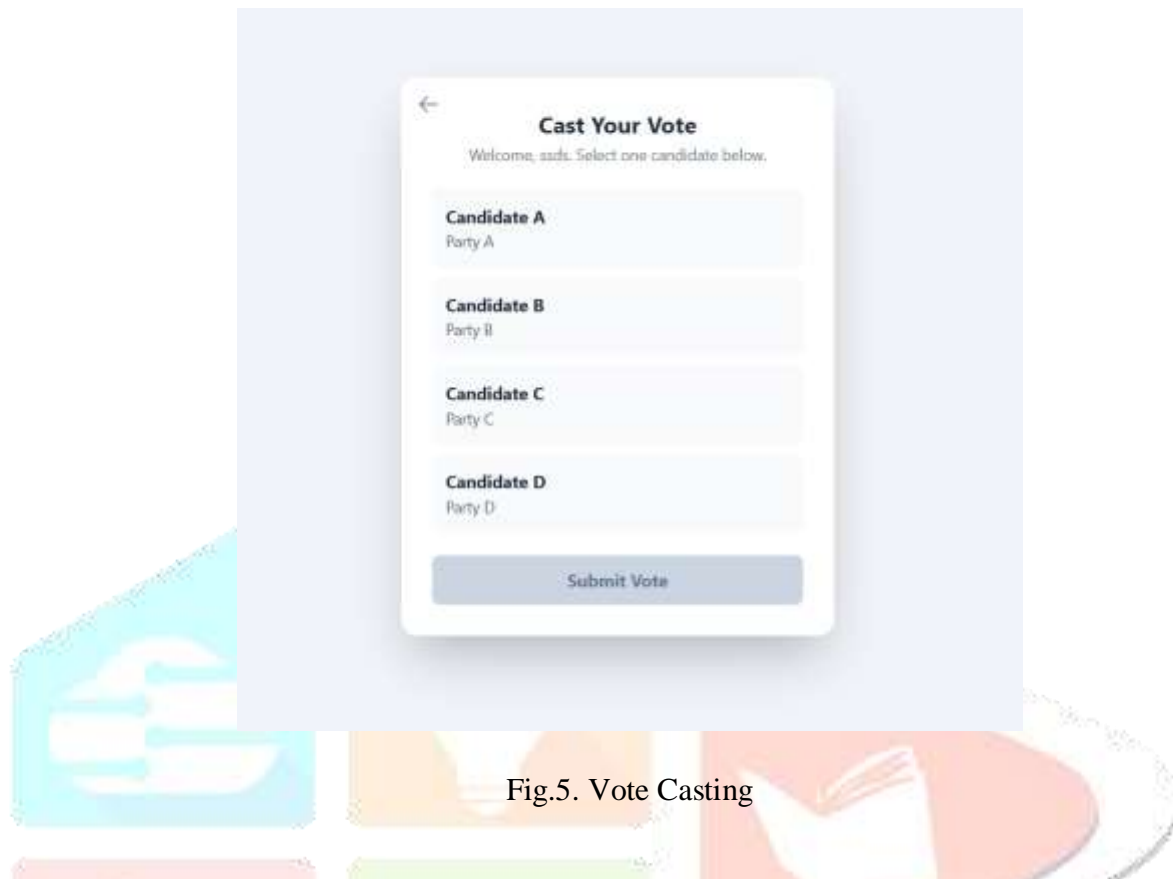


Fig.5. Vote Casting

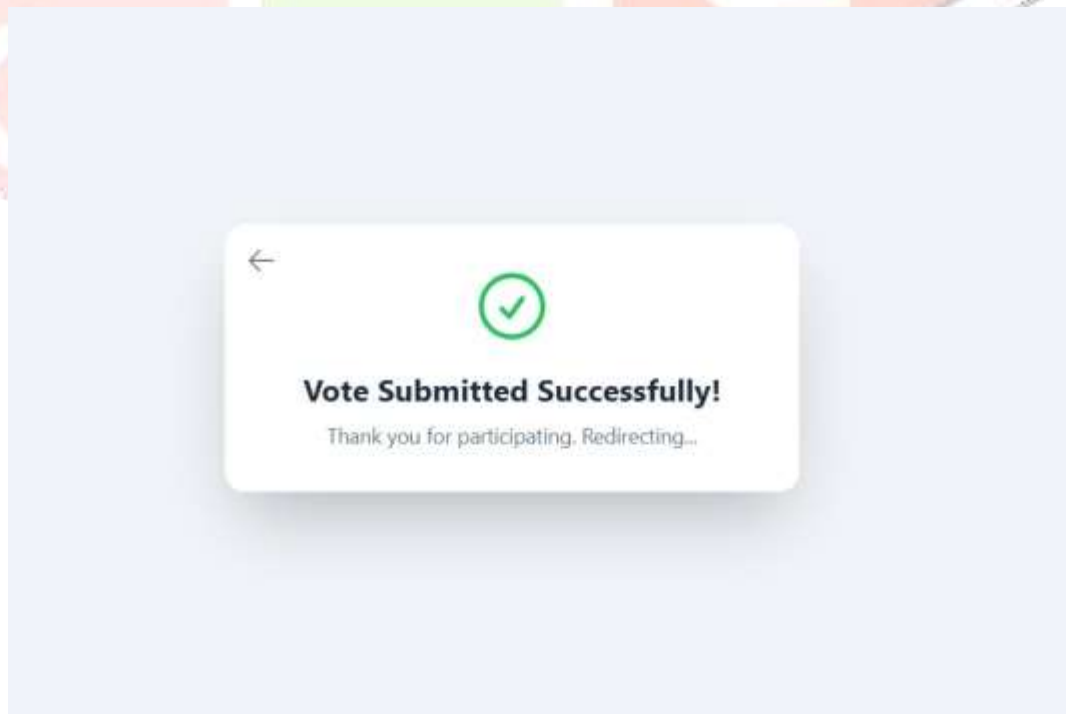


Fig.6. Vote Submitted

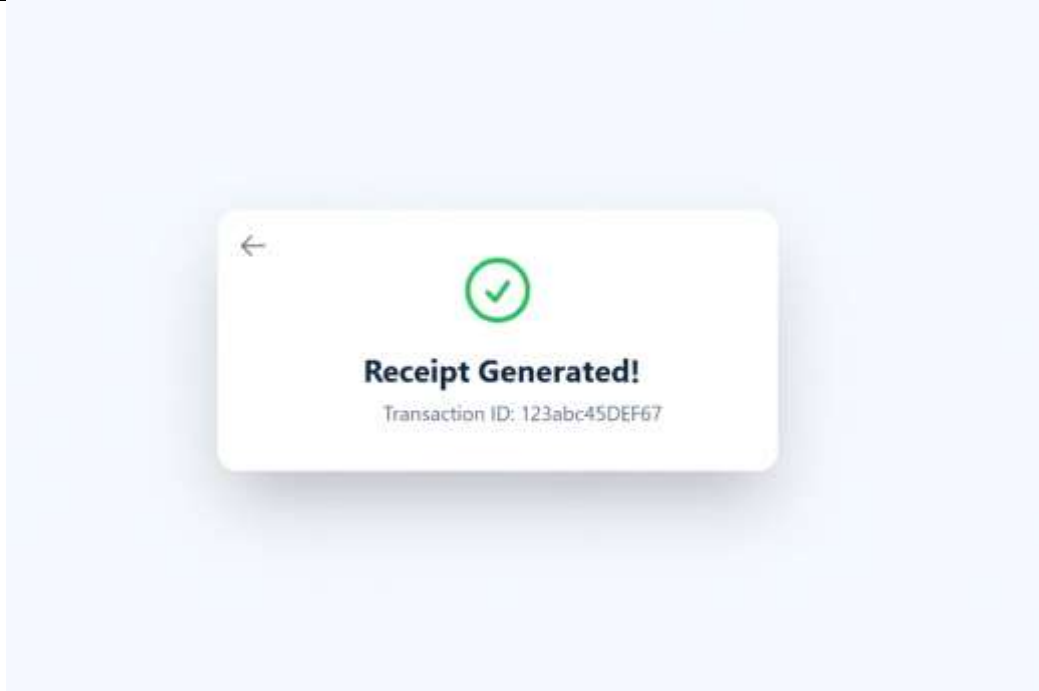


Fig.7. Receipt Generated

Conclusion:

The fingerprint-based secure e-voting system successfully shows how biometric authentication can strengthen the security and trustworthiness of digital elections. By verifying each voter through their fingerprint and encrypting both biometric data and votes, the system ensures that only legitimate voters participate and every vote remains confidential and tamper-proof. The voting process becomes faster, more accurate, and far more transparent compared to traditional methods. The system also enhances user confidence through receipt generation, allowing voters to confirm their participation without revealing their choices. Overall, this work demonstrates that integrating biometrics with secure data handling provides a practical and reliable foundation for modern e-voting solutions.

Future Work:

Although the system performs effectively, several improvements can be explored in future versions. Additional biometric traits such as iris or facial recognition could be integrated to create a multi-factor authentication system, further increasing security. Implementing blockchain more deeply into the vote-storage layer can help create a fully decentralized and tamper-proof audit trail. The user interface can also be refined to support larger-scale elections and multilingual accessibility. Finally, real-world deployment tests involving larger datasets and diverse environmental conditions would help validate the system's robustness and adaptability. These enhancements can contribute to making the e-voting system even more secure, scalable, and user-friendly in the future.

References

- [1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.
- [2] S. Tiwari and P. Yadav, "Fingerprint-based voter identification for secure e-voting," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 123–128, 2017.
- [3] S. Kumar and A. Sharma, "Biometric e-voting system using AES encryption," *International Journal of Computer Engineering and Technology*, vol. 10, no. 3, pp. 78–85, 2019.
- [4] N. Ahmed and K. Farooq, "Secure electronic voting using RSA-based cryptography," *International Journal of Network Security*, vol. 12, no. 4, pp. 256–264, 2018.
- [5] M. Aditya and P. Saha, "Blockchain-based biometric e-voting: Ensuring anonymity and integrity," *International Journal of Computer Science and Information Security*, vol. 17, no. 6, pp. 84–91, 2019.
- [6] J. Feng, "Minutiae-based fingerprint matching algorithms," *Pattern Recognition*, vol. 43, no. 3, pp. 1148–1158, 2010.
- [7] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2009.
- [8] P. Gupta and R. Bansal, "Enhanced preprocessing for fingerprint recognition using noise reduction and feature extraction," *International Journal of Biometrics*, vol. 7, no. 2, pp. 147–162, 2015.

