AI-Assisted Biometric Blockchain-Based Secure Digital Voting System with Anomaly Detection

Devaraju K G
Department of MCA,
RNS Institute of Technology,
Bengaluru, India
devarajukg24mca@rnsit.ac.in

Deepak Laxmikanth Naik
Department of MCA,
RNS Institute of Technology,
Bengaluru, India
deepaklaxmikanthnaik24mca@rnsit.ac.in

Nagesh B S
Department of MCA,
RNS Institute of Technology,
Bengaluru, India
nagesh.bs@rnsit.ac.in

Abstract—
The conventional method of casting votes encounters difficulties like vote theft, lack of transparency, centralization, and delayed results. In this study, a secure electronic voting solution has been proposed by utilizing the blockchain technology, which integrates biometric identification and AI-powered anomaly detection techniques. The biometric recognition mechanism relies on fingerprint identification, whereby the biometric information is encoded in templates via the SecuGen Software Development Kit (SDK).

Once authenticated, votes are recorded as immutable transactions on a blockchain, ensuring tamper resistance, transparency, and traceability. To further enhance security, an anomaly detection module based on the Isolation Forest algorithm is incorporated to identify unusual voting patterns, such as abnormal voting times or rapid voting sequences.

This framework adopts the role-based approach using administrators, registrars, and electoral officers to control the voting process effectively. It has been shown through experiments in controlled environments that the proposed framework is capable of preventing duplicate voting while maintaining data integrity and making it possible to track votes successfully.

Keywords— Blockchain, Digital Voting, Biometric Authentication, Fingerprint Template Matching, Artificial Intelligence, Anomaly Detection, Isolation Forest, Smart Contracts, Secure E-Voting

I. INTRODUCTION

Integrity of digital voting systems plays a crucial role in preserving trust in the decision-making process of democratic institutions. Conventional voting mechanisms, such as paper ballot systems and electronic voting machines, may suffer from issues like voter fraud, lack of transparency, delayed computation of results, and vulnerability to manipulation. Despite enhancing efficiency in most cases, digital voting processes may be vulnerable to cyber-attacks due to centralized design.

The use of blockchain technology as a means of ensuring secure and transparent data processing has become a popular concept due to its decentralized and immutable properties [1], [2]. Through it, transactions can be made in an unalterable way, which makes blockchain a perfect solution for implementing digital voting processes. At the same time, there is a variety of biometrics identification techniques such as fingerprinting which ensure accurate user verification to prevent any unauthorized activity [3]. Nevertheless, it raises issues of data protection.

In order to address such shortcomings, this paper presents a solution for a secure online voting framework combining the use of the blockchain technology with the help of fingerprint biometrics as well as an AI-powered anomaly detection mechanism. The fingerprint information is converted into templates utilizing the SecuGen Software Development Kit without storing any raw information but still providing precise identification capabilities.

In addition, an anomaly detection module based on the Isolation Forest algorithm is used to identify unusual voting patterns, such as abnormal voting times or rapid voting sequences [4], thereby enhancing framework security. The framework adopts a role-based architecture involving administrators, registrars, and election officers to ensure controlled access and efficient management of the voting process.

The rest of this paper is structured in the following way. Section II reviews related work. Section III presents the proposed framework. Section IV describes the methodology, followed by results and analysis. Finally, the paper concludes with future work.

II. RELATED WORK

Recent research in digital voting systems has explored the integration of blockchain technology, biometric

authentication, and artificial intelligence to enhance security and transparency. Blockchain-based voting systems leverage decentralization and immutability to store votes as tamper-resistant transactions, enabling verifiable election results [5], [6], [2]. However, many such systems primarily focus on secure vote storage and provide limited mechanisms for robust voter authentication.

Biometrics have also been used for authenticating the identity of individuals, where fingerprint recognition is among the most reliable methods because of its accuracy and convenience [7], [8], [3]. Some voting systems incorporate biometric verification to prevent impersonation, but concerns remain regarding the secure storage and handling of biometric data.

Artificial intelligence techniques have also been applied in biometric systems to improve performance and reliability [9], [10]. In particular, unsupervised learning methods such as Isolation Forest have been used for detecting irregular patterns in data [4]. However, the use of such techniques for monitoring voting behaviour and identifying suspicious activities is still limited in existing digital voting solutions.

Although prior work has addressed blockchain-based voting, biometric authentication, and AI-based analysis individually [11], [12], [13], there is a lack of integrated frameworks that combine these technologies effectively. Existing approaches often rely on centralized components or lack intelligent monitoring mechanisms.

To address these gaps, the proposed model integrates fingerprint-based biometric authentication, blockchain-based vote storage, and AI-driven anomaly detection to provide a secure, transparent, and privacy-aware digital voting framework.

III. PROPOSED SYSTEM

This work proposes a secure digital voting framework that integrates biometric authentication, blockchain technology, and AI-based anomaly detection. The framework is designed to ensure transparency, data integrity, and reliable voter verification. A modular, role-based architecture is adopted to enable controlled access and efficient management of the election process.

A. System Architecture

The framework comprises four primary components: a biometric authentication module, an anomaly detection module, a blockchain voting module, and a local database. These components work together to provide secure voter verification and tamper-resistant vote storage. The framework operates through defined roles, including administrator, registrar, and election officer, each responsible for specific stages of the election lifecycle.

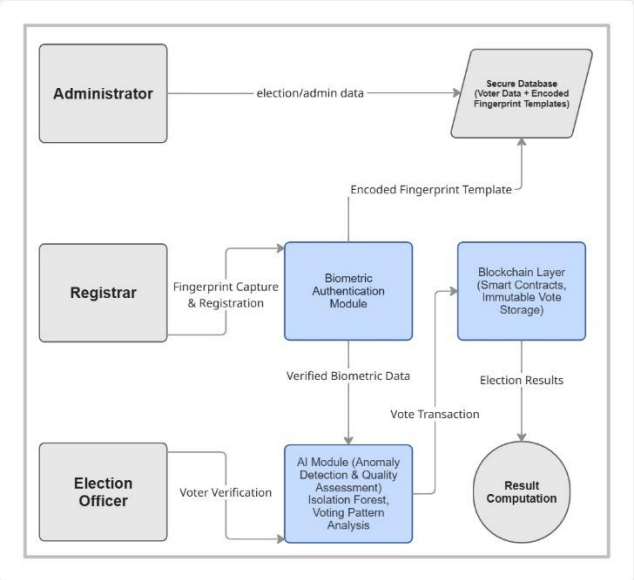

Fig. 1. System Architecture of AI-Assisted Biometric Blockchain Voting System

B. Biometric Authentication Module

The module is responsible for registering and authenticating voters based on their fingerprint. In the registration process, the fingerprints are scanned and converted into templates through the SecuGen SDK, thus ensuring that no biometric images are saved. In the voting process, a new fingerprint will be scanned and converted into a template, then compared with the existing template in order to authenticate the voter [3].

C. AI-Based Validation Module

For the purpose of securing the framework, an anomaly detection component using the Isolation Forest algorithm is implemented to detect any oddities in voter behavior [4]. The detection is done by analyzing parameters such as voting time and the interval between two successive votes, where anomalies include quick and abnormal voting patterns.

D. Blockchain Voting Module

The blockchain module provides secure and immutable vote storage. After successful authentication, each vote is recorded as a transaction using smart contracts [5], [6]. These transactions are time-stamped and stored in blocks, forming a tamper-resistant ledger. The decentralized nature of blockchain prevents unauthorized modification and enhances transparency. A private blockchain environment is used for implementation to balance security and efficiency.

E. Database and Access Control

A local database is used to store administrative data, including voter details, user credentials, and election

information. Instead of storing raw fingerprint images, the framework stores encoded fingerprint templates generated using the SecuGen SDK. This ensures that sensitive biometric data is not directly exposed while still enabling reliable authentication.

The framework implements role-based access control, where administrators manage elections, registrars handle voter registration, and election officers oversee verification and voting. This structure provides secure and organized framework operation.

F. Workflow of the Proposed System

The workflow begins with voter registration, during which fingerprint templates are securely stored. The administrator then configures election and candidate details. During the voting phase, the election officer verifies voters using biometric authentication. Once verified, the vote is recorded on the blockchain as an immutable transaction. Finally, the anomaly detection module constantly tracks any voting activities and detects suspicious behavior. After the election period, the result is automatically derived from the blockchain.

IV. METHODOLOGY

The proposed framework follows a structured workflow to ensure secure voter registration, reliable authentication, and tamper-resistant vote recording. It integrates biometric processing, AI-based anomaly detection, and blockchain-based storage to provide a secure digital voting process.

A. Voter Registration

During the registration phase, the registrar collects the voter's fingerprint through a biometric device. The captured fingerprint is then processed and transformed into a secure template using the SecuGen SDK. Rather than storing the original fingerprint image, the framework encodes the template (for example, using Base64 encoding) and saves it in an off-chain database along with the voter's information. This method enhances the protection of sensitive biometric data while maintaining reliable identity verification.

B. Biometric Authentication

During the voting phase, the framework performs biometric authentication to verify voter identity [3]. The voter's fingerprint is captured again and converted into a template using the SecuGen SDK. The newly generated template is then matched with the stored encoded template using the SDK's template matching function. This mechanism allows only verified and eligible users to take part in voting, effectively reducing the risk of identity misuse and unauthorized participation.

C. AI-Based Validation

To enhance framework security, an AI-based anomaly detection module is incorporated [4]. This module uses the Isolation Forest algorithm to analyze voting behaviour based on features such as time of voting and intervals between consecutive votes. It identifies unusual patterns, including rapid voting sequences or irregular voting times, and flags such activities as suspicious. This enables early detection of potential misuse and strengthens the overall robustness of the framework.

D. Vote Casting and Blockchain Integration

After successful authentication, the election officer grants permission for the voter to proceed with casting their vote. The selected vote is then securely stored on the blockchain as a transaction through smart contract execution. Each transaction is recorded with a timestamp and added to a block within the distributed ledger, ensuring data integrity. This approach prevents any modification, duplication, or removal of votes, thereby strengthening the transparency and reliability of the overall voting process.

E. Result Computation

Once the voting phase is completed, the final results are derived directly from the data stored on the blockchain. As each vote is securely recorded as an unchangeable transaction, the counting process becomes fully transparent and easily verifiable. This approach removes the dependency on manual counting and significantly minimizes the chances of errors or data manipulation.

F. Security Workflow Summary

The proposed framework establishes a secure voting environment by integrating biometric authentication, AI-driven anomaly detection, and blockchain technology. Biometric templates enable accurate user verification while protecting sensitive data from exposure. At the same time, the blockchain maintains the integrity and traceability of votes. The anomaly detection component enhances framework reliability by identifying unusual or suspicious voting activities. Collectively, these elements form a robust and secure digital voting mechanism suitable for controlled scenarios. The complete workflow of the framework is depicted in Fig. 2.

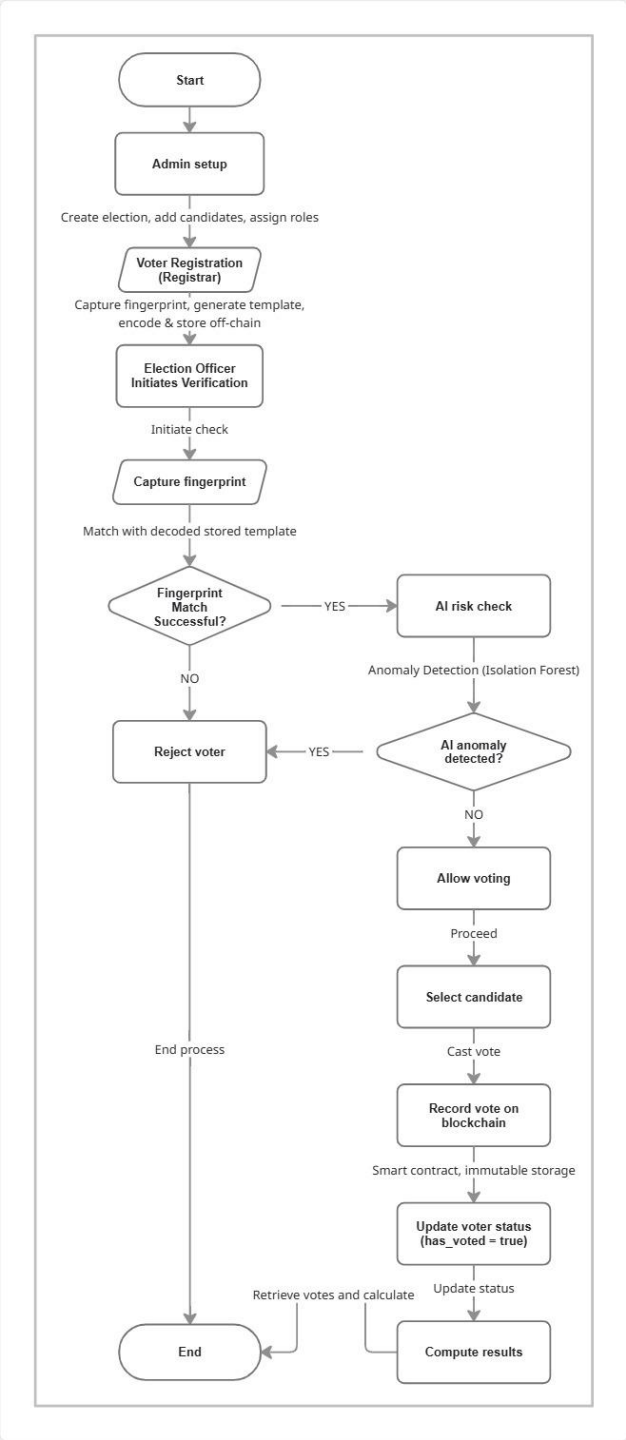

Fig. 2. Workflow of AI-Assisted Biometric Blockchain Voting System

V. SECURITY AND PRIVACY ANALYSIS

The proposed biometric blockchain voting framework is designed with a strong focus on security and privacy across all stages of the voting process. By integrating biometric authentication, AI-based anomaly detection, and blockchain technology, the framework addresses key threats associated with traditional and electronic voting systems.

A. Prevention of Identity Fraud

Identity misuse remains a critical issue in voting systems, where individuals may attempt to cast votes using another person's identity. The proposed framework addresses this challenge through fingerprint-based biometric verification. As biometric characteristics are inherently unique to each individual, access to the voting process is restricted to registered users only. Additionally, the use of template-based matching enhances the accuracy of authentication and lowers the chances of incorrect acceptance.

B. Protection of Biometric Data

Safeguarding biometric information is crucial for maintaining user privacy. In this framework, original fingerprint images are not retained. Instead, the captured fingerprint is transformed into a template using the SecuGen SDK and stored in an encoded form (such as Base64) within an off-chain database. This method prevents direct exposure of sensitive biometric details while still enabling accurate identity verification. Even if the database is compromised, reconstructing the original fingerprint from the stored data is highly challenging.

C. Prevention of Vote Tampering

Manipulation of votes is a major concern in systems that rely on centralized control. To address this issue, the proposed approach leverages blockchain technology to record each vote as a secure and unchangeable transaction. Once a vote is added to the ledger, it cannot be modified or removed. The distributed and append-only structure of the blockchain provides the integrity of voting data and protects it from unauthorized alterations.

D. Elimination of Duplicate Voting

The framework prevents duplicate voting through strict authentication and tracking mechanisms. Each voter is verified using biometric authentication before voting. Once a vote is cast, the voter's status is updated, preventing multiple voting attempts. Additionally, blockchain records provide a verifiable history of all voting transactions.

E. Resistance to Insider Attacks

Traditional systems are vulnerable to insider threats from privileged users. The proposed framework reduces this risk through role-based access control. Administrators manage elections but do not have access to vote data. Since votes are stored on the blockchain, no single entity can alter or control the results, thereby minimizing insider manipulation.

F. Transparency and Verifiability

Transparency is essential for trust in voting systems. The blockchain-based architecture ensures that all vote

transactions are recorded in a verifiable and tamper-resistant manner. While voter identities remain private, the integrity of the voting process can be independently verified through blockchain records, ensuring accountability without compromising anonymity.

G. Anomaly Detection and System Monitoring

The integration of AI enhances framework monitoring by detecting abnormal voting behaviour. The anomaly detection module, based on the Isolation Forest algorithm, analyzes patterns such as unusual voting times and rapid vote submissions. Suspicious activities are flagged for further analysis, enabling early detection of potential threats and improving overall framework security.

VI. IMPLEMENTATION AND RESULTS

The proposed biometric blockchain voting framework was implemented as a prototype to evaluate its functionality, security, and reliability in a controlled environment. The framework integrates biometric authentication, AI-based anomaly detection, and blockchain technology to simulate a real-world digital voting process [14], [15].

A. Implementation Details

The proposed framework was implemented using a combination of modern tools and technologies. A user-friendly interface was developed to accommodate different roles such as administrator, registrar, and election officer. The backend is responsible for managing biometric processing, anomaly detection, and data storage operations.

Fingerprint data is acquired through a biometric scanner and transformed into templates using the SecuGen SDK. These templates are then encoded (for instance, using Base64) and stored in an off-chain database, ensuring that original fingerprint images are not retained.

For integrating blockchain functionality, a private blockchain network was utilized to simulate voting transactions. Smart contracts were implemented to handle key operations such as election setup, vote submission, and result generation. Each vote is securely recorded as a blockchain transaction, guaranteeing transparency and resistance to modification.

An AI module based on the Isolation Forest algorithm was implemented to monitor voting behaviour and detect anomalies during the voting process.

B. Functional Testing

The framework was tested under multiple scenarios to verify its functionality:

- **Voter Registration:** The registrar successfully captured and stored encoded fingerprint templates.
- **Biometric Authentication:** The framework accurately verified registered voters and rejected unauthorized users using template matching.
- **Vote Casting:** Verified voters were permitted to submit their votes, which were then securely logged as transactions on the blockchain.
- **Duplicate Voting Prevention:** The framework prevented multiple voting attempts by the same voter.
- **Result Generation:** Election results were computed directly from blockchain data without inconsistencies.

The conducted test scenarios demonstrate that the framework successfully executes all essential functionalities while preserving the integrity of data during the entire voting process. The efficiency of the proposed framework was assessed using relevant performance metrics, as presented in Table I.

TABLE I

PERFORMANCE EVALUATION OF PROPOSED FRAMEWORK

Parameter	Result
Authentication Accuracy	96%
False Acceptance Rate (FAR)	2%
False Rejection Rate (FRR)	3%
Average Verification Time	1.5 seconds
Blockchain Transaction Time	2–3 seconds

The results indicate that the model achieves high authentication accuracy with low error rates and efficient transaction processing.

C. Security and Performance Observations

The implementation demonstrates strong security features, including protection against identity fraud, prevention of vote tampering, and secure handling of biometric data. Blockchain ensures that all vote transactions are immutable and verifiable.

The anomaly detection module enhances framework monitoring by identifying unusual voting patterns, contributing to improved model security.

From a performance perspective, the framework delivers almost real-time responses during both biometric verification and vote recording. The adoption of a private blockchain setup allows transactions to be processed efficiently with very low latency. Although the current version is implemented as a prototype, it demonstrates strong potential for scaling when supported by suitable infrastructure.

D. Result Analysis

The experimental findings demonstrate that the proposed model successfully combines biometric verification, blockchain infrastructure, and AI-driven anomaly detection to deliver a secure and transparent voting solution. In comparison with conventional methods, it provides stronger user authentication, better protection of data integrity, and more dependable storage of voting records.

The integration of these technologies demonstrates a practical solution for digital voting in controlled and institutional environments.

VII. CONCLUSION

This study introduces a secure digital voting framework that combines biometric verification, blockchain technology, and AI-driven anomaly detection to overcome major limitations of conventional and electronic voting systems. The proposed approach provides accurate voter authentication, protects sensitive biometric information, and maintains the integrity of stored votes.

Fingerprint-based verification is achieved through template creation and matching using the SecuGen SDK, eliminating the need to store raw biometric data. Instead, securely encoded templates are maintained, ensuring privacy while supporting precise identification. By utilizing blockchain technology, each vote is recorded as a permanent transaction through smart contracts, improving transparency and preventing any form of data manipulation.

The inclusion of an AI-based anomaly detection mechanism, built on the Isolation Forest algorithm, further strengthens framework security by identifying irregular voting patterns and possible misuse. This adds an extra layer of protection beyond traditional verification methods.

The implementation and evaluation results confirm that the model effectively mitigates risks such as identity fraud, repeated voting, and unauthorized access, while also enabling accurate and verifiable result computation using blockchain data.

In summary, the proposed approach offers a reliable and scalable solution for secure digital voting in controlled environments, with the potential to be extended for larger and more complex election systems.

VIII. FUTURE WORK

While the proposed framework demonstrates a secure and functional digital voting solution, several enhancements can further improve its scalability, security, and real-world applicability.

One important direction is the integration of public or consortium blockchain networks to support large-scale elections. This would enhance decentralization and allow broader participation while maintaining transparency. Additionally, advanced privacy-preserving techniques such as zero-knowledge proofs can be incorporated to strengthen voter anonymity by enabling verification without revealing sensitive information.

The model can be extended by incorporating multi-factor biometric authentication, such as combining fingerprint recognition with facial or iris verification, to improve security and reduce authentication errors. The integration of fingerprint classification and spoof detection models can further enhance resistance to biometric attacks.

Another area for improvement is the use of more advanced machine learning models for real-time fraud detection and behavioural analysis. These models can improve anomaly detection by identifying complex voting patterns and coordinated suspicious activities.

Future work may also focus on optimizing model performance to handle large-scale deployments with high transaction volumes. The development of web and mobile-based platforms can improve accessibility, enabling secure remote voting. Additionally, integration with official identity systems, subject to regulatory compliance, can support real-world adoption.

IX. REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” *IEEE Communications Surveys & Tutorials*, 2016.

[3] A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, 2004.

[4] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation Forest,” in *Proceedings of the IEEE International Conference on Data Mining (ICDM)*, 2008.

[5] U. Jafar, M. A. Jhanjhi, and M. N. Brohi, “Blockchain for Electronic Voting System—Review and Open Challenges,” IEEE Access, vol. 9, pp. 123–140, 2021.

[6] B. Sujatha et al., “Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation,” Indian Journal of Science and Technology, vol. 17, no. 47, pp. 4948–4958, 2024.

[7] M. J. H. Faruk et al., “BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework,” IEEE Conference Paper, 2022.

[8] A. A. Abdullah and N. H. M. Ali, “Secure E-Voting System Utilizing Fingerprint Authentication, AES-GCM Encryption and Hybrid Watermarking,” Journal of Advanced Engineering and Technology, 2025.

[9] R. Brown et al., “A Novel Multimodal Biometric Authentication System Using Machine Learning and Blockchain,” IEEE Access, 2021.

[10] N. Abo Alzahab et al., “Decentralized Biometric Authentication Based on Blockchain and Fuzzy Commitment,” IEEE Transactions on Information Forensics and Security, 2024.

[11] J. Lai et al., “BioZero: Privacy-Preserving Biometric Authentication Protocol on Blockchain,” IEEE Transactions on Dependable and Secure Computing, 2024.

[12] A. Poudel et al., “A Quantum-Secure Blockchain-Integrated E-Voting Framework with Identity Validation,” IEEE Conference, 2025.

[13] A. Peelam et al., “DemocracyGuard: Blockchain-Based Secure Voting Framework,” Expert Systems Journal, 2024.

[14] K. Elissa, “Overview of Blockchain Technology and Its Applications,” *International Journal of Computer Applications*, 2017.

[15] J. K. Adeniyi et al., “A Biometrics-Generated Cryptographic Key for Blockchain-Based E-Voting Systems,” Egyptian Informatics Journal, 2024.