International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 15 Issue 3, March-2026

"Blockchain Integration with Multimodal Biometric Authentication System for Secure Smart Verifiable Electronic Voting System"

Ms. Yogita Chhagan Ghangurdde[1], Dr. Anand Khatri[2],
Prof. Sachin Bhosale[3], Dr. Shubhangi Gunjal[4]

[1]Student, Department of Artificial Intelligence and Data Science Engg, Jaihind College of Engineering
[2]Professor, Department of Artificial Intelligence and Data Science Engg, Jaihind College of Engineering,
[3]Professor, Department of Artificial Intelligence and Data Science Engg, Jaihind College of Engineering,
[4]Professor &HOD, Department of Artificial Intelligence and Data Science Engg, Jaihind College of Engineering,
Pune, Maharashtra, India

ABSTRACT

Ensuring transparency, security, and trust in electronic voting systems remains a critical challenge in modern digital democracies. Conventional e-voting platforms often rely on centralized infrastructures and single-factor authentication mechanisms, which increase vulnerability to impersonation, insider manipulation, and data tampering. This research proposes an artificial intelligence-driven multimodal biometric authentication system integrated with blockchain technology to establish a secure and verifiable electronic voting framework. The system combines facial recognition using convolutional neural network-based feature extraction and voice authentication using MFCC-based signal analysis to strengthen voter identity validation.

Upon successful authentication, each vote is encrypted, cryptographically hashed, and recorded through Ethereum smart contracts on a distributed blockchain ledger. The decentralized architecture eliminates single points of failure while ensuring data integrity, auditability, and resistance to unauthorized modification. The proposed framework aims to enhance voter privacy, enforce single authenticated ballot submission, and provide a scalable architecture suitable for secure institutional and governmental election environments.

Keywords: Multimodal Biometric Verification, Blockchain-Based Voting, Smart Contract Security, Distributed Election Framework, Facial Recognition, Voice Authentication, Cryptographic Hashing, Decentralized Governance Systems.

INTRODUCTION

The rapid growth of digital governance has encouraged the exploration of secure electronic voting mechanisms capable of supporting transparent and efficient democratic processes. While traditional paper-based elections ensure physical verifiability, they often involve high operational cost, manual effort, and delayed result processing. In contrast, electronic voting platforms offer speed and accessibility but introduce significant security and trust challenges. Many existing e-voting systems are built on centralized infrastructures where authentication, vote storage, and result computation are managed by a single authority. Such architectures increase exposure to insider threats, database manipulation, denial-of-service attacks, and system compromise. Additionally, single-factor authentication methods such as passwords or ID verification are insufficient for high-security electoral environments.

To address these limitations, this research proposes a distributed voting framework that integrates artificial intelligence-based multimodal biometric authentication with blockchain-backed vote recording. The system employs facial recognition using deep learning-based feature extraction and voice authentication using signal processing techniques to ensure robust voter identity validation. By combining multiple biometric modalities, the probability of impersonation and spoofing attacks is significantly reduced. Blockchain technology is utilized to record encrypted vote transactions through smart contracts. Once stored on the distributed ledger, vote data becomes computationally impractical to alter, thereby strengthening transparency and auditability. The integration of biometric authentication with decentralized vote storage enables a secure, privacy-preserving, and tamper-resistant electronic voting architecture suitable for institutional and governmental application.

Motivation

The motivation behind this research arises from the increasing need for secure, transparent, and trustworthy digital election systems in modern democratic environments. As societies adopt digital platforms for governance and public services, traditional voting mechanisms face limitations in scalability, remote accessibility, and operational efficiency. At the same time, existing electronic voting solutions often suffer from centralized control structures, weak authentication mechanisms, and limited audit transparency, which reduce public trust. Another significant motivation is the growing concern regarding identity fraud, impersonation, and vote manipulation in digital systems.

Single-factor authentication methods such as passwords or ID verification are insufficient for high-security electoral applications. Strengthening voter identity validation through multimodal biometric techniques can significantly reduce the risk of unauthorized participation. Furthermore, the integration of blockchain technology provides an opportunity to enhance election integrity by enabling distributed vote recording, cryptographic verification, and tamper resistance. By combining artificial intelligence-based biometric authentication with decentralized ledger technology, the proposed framework aims to create a secure, privacy-preserving, and verifiable electronic voting architecture capable of supporting future-ready democratic processes.

Objectives

The primary objective of this research is to develop a secure blockchain-integrated electronic voting framework supported by artificial intelligence-based multimodal biometric authentication. The specific objectives are:

- To develop a distributed blockchain-based vote recording architecture ensuring cryptographic integrity and resistance to unauthorized modification.
- To design and integrate a multimodal biometric authentication mechanism combining facial recognition and voice verification for secure voter identity validation.
- To implement smart contract-driven automated ballot validation and encrypted vote storage.
- To establish a decentralized audit mechanism enabling transparent verification of recorded transactions.
- To create a modular and scalable system architecture suitable for institutional and governmental deployment.

PROPOSED FRAMEWORK

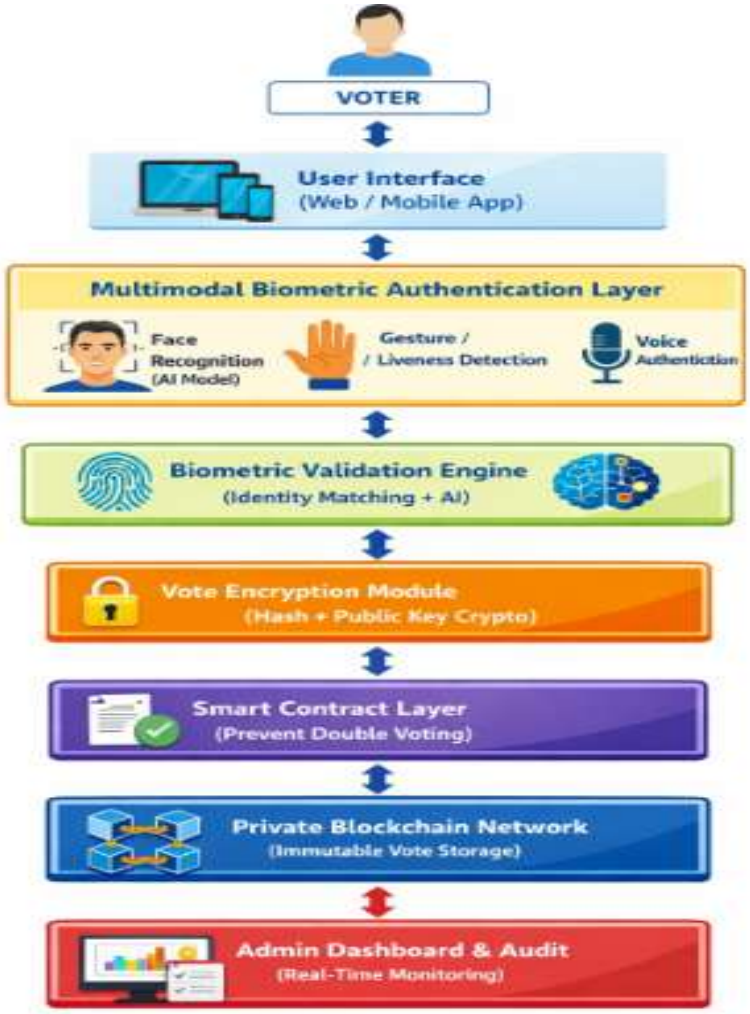
The proposed framework is designed as a secure, modular, and scalable electronic voting architecture that integrates multimodal biometric authentication with blockchain-based vote recording. The system operates through a structured workflow beginning with voter enrollment, followed by biometric verification, ballot submission, smart contract validation, and distributed ledger storage.

The framework separates authentication, vote processing, and blockchain recording into independent yet interconnected modules. This modular approach enhances maintainability, scalability, and fault tolerance. By combining artificial intelligence-driven identity verification with decentralized ledger technology, the system reduces reliance on centralized authorities and strengthens election integrity.

Each verified voter session is granted controlled access to ballot submission, ensuring single authenticated vote casting. Once a vote is submitted, it is encrypted, hashed, and transmitted to the blockchain network through smart contract execution, preventing unauthorized modification.

3.1 System Architecture.

The proposed system is designed using a layered architecture model that integrates multimodal biometric authentication with blockchain technology to ensure secure, transparent, and verifiable electronic voting.



Voter Layer

The process begins with the registered voter who accesses the system using a web or mobile device. Only pre-enrolled voters stored in the secure database are allowed to proceed further in the workflow.

User Interface (Web/Mobile App): This module acts as the interaction layer between the voter and backend system.

Functions:

- Provides login access
- Displays authentication instructions
- Shows ballot page
- Gives real-time feedback

It securely connects to backend modules without storing vote data.

Multimodal Biometric Authentication Layer: This layer verifies voter identity using multiple biometric inputs

- Face Recognition – AI-based facial feature matching
- Gesture/Liveness Detection – Confirms real human presence
- Voice Authentication – Verifies speaker identity

Access is granted only if all biometric checks are successfully validated.

1. **Biometric Validation Engine**.
   This module:

- Compares captured biometric data with registered templates
- Calculates matching scores
- Applies confidence threshold

If validation fails → Access denied
If successful → Vote casting allowed

2. **Vote Encryption Module:** After authentication, the selected vote is:
- Converted into encrypted format
- Assigned a unique hash value
- Secured using cryptographic algorithms

This ensures confidentiality before blockchain storage.

3. **Smart Contract Layer:** Smart contracts automatically:
- Verify voter eligibility
- Prevent double voting
- Enforce election rules
- Validate transaction logic

This eliminates manual intervention.

4. **Private Blockchain Network:** Encrypted votes are stored as blockchain transactions.

Blockchain ensures:
- Immutability
- Tamper resistance
- Transparency
- Decentralized storage

Once stored, votes cannot be modified

5. **Admin Dashboard & Audit Layer:** Authorized officials can:
- Monitor real-time voting progress
- Verify blockchain records
- Generate result reports

Admin cannot alter vote data, ensuring fairness.

3.2 System Features

The proposed blockchain-integrated multimodal biometric voting system offers a wide range of advanced features designed to enhance security, transparency, and usability:

The key features of the system are as follows:

- **Multimodal Biometric Authentication:** combines face and voice recognition to improve authentication accuracy and reduce spoofing attacks..
- **Decentralized Blockchain Storage** Eliminates centralized control and ensures tamper-proof vote records.
- **Smart Contract Integration:** Automatically validates votes and enforces one-person-one-vote policy..
- **End-to-End Verifiability** Allows verification of election results without compromising voter privacy
- **Secure Encryption Mechanism** Protects biometric data and vote content using cryptographic techniques.
- **User-Friendly Interface:** Provides a simple and accessible voting experience.
- **Audit and Transparency Support:** Enables authorized auditing through immutable blockchain records.

3.2.1 Feasibility

The feasibility of the Intelligent Gesture-Enhanced Blockchain Voting System has been analyzed based on technical, operational, and economic aspects. The system is designed using easily available technologies and open-source tools, making it practical and cost-effective for real-world implementation.

a) Technical Feasibility

The system can be implemented using existing technologies such as artificial intelligence models for biometric recognition, blockchain platforms for decentralized storage, and secure web/mobile development frameworks. Required hardware components like cameras and microphones are commonly available in modern devices, making deployment technically achievable. Open-source libraries and development tools further simplify implementation

b) Operational Feasibility

The system is designed with a user-friendly interface and guided workflow, enabling voters to interact with minimal technical knowledge. Administrative monitoring tools allow election authorities to manage and supervise the process efficiently. The integration of automated smart contracts reduces manual workload and operational complexity.

c) **Economic Feasibility**

The use of digital infrastructure reduces costs associated with physical ballot printing, transportation, and manual counting. A permissioned blockchain network minimizes infrastructure expenses compared to large public networks. Overall, the system provides a cost-effective and scalable solution for institutional or governmental elections.

3.2.2 Usability

The proposed system is designed with a user-friendly and accessible interface to ensure smooth interaction for voters with varying technical backgrounds. Clear on-screen instructions and real-time feedback guide users through biometric authentication and vote submission. The use of facial and voice verification eliminates the need for passwords or PINs, simplifying the authentication process. The interface is adaptable to different devices and environmental conditions, supporting efficient and inclusive participation in digital elections.

User Interface Design:
The user interface is designed to be clean, intuitive, and easy to use. Clear on-screen instructions and real-time visual feedback guide users through the voting process, ensuring smooth navigation and reducing user confusion across different devices.

Ease of Learning:
The system is easy to learn and use, requiring minimal training. Users can quickly understand gesture controls through visual cues and on-screen instructions, making the voting process simple, efficient, and accessible to all.

Efficiency of Use:
The system ensures fast and seamless operation with real-time gesture recognition and quick blockchain validation. Users can cast votes securely within seconds, reducing waiting time and improving overall voting efficiency.

Error Prevention and Recovery:
The system minimizes user errors through guided prompts and gesture validation. If an incorrect gesture or input is detected, it immediately notifies the user and allows retrying without restarting the process, ensuring a smooth and error-free voting experience.

Accessibility and Responsiveness:
The system is designed to be inclusive and responsive across all devices. Gesture control enables participation by differently-abled users, while the adaptive interface adjusts to various screen sizes and lighting conditions, ensuring smooth interaction and real-time responsiveness.

CONCLUSION

The proposed Blockchain- Integrated Multi-modal Biometric Electronic Voting System enhances security, transparency, and trust in digital elections. The integration of AI-based biometric authentication and blockchain technology ensures secure voter verification and tamper-resistant vote storage. Similar approaches have demonstrated improved integrity and reliability in electronic voting systems [1]. Therefore, the proposed architecture provides a scalable and secure solution for modern election environments.

FUTURE WORK

While the current implementation provides a robust and effective underwater image enhancement system, several improvements can be made in future versions to expand its capabilities and performance.

1. Real-Time Enhancement:
Future work will focus on achieving faster and more precise gesture recognition by optimizing AI models for real-time response and minimal latency during live voting sessions.

2. Multi-Model Integration:
Combining gesture, facial, and voice recognition can create a robust multi-factor authentication system that strengthens security and ensures accurate voter identification.

3. Dataset Expansion and Domain Adaptation:
Expanding datasets with diverse user samples and adapting models to various environments will improve performance under different lighting, camera angles, and cultural gesture variations.

4. Mobile and Edge Deployment:
Deploying the system on mobile and edge platforms will allow users to participate securely from personal devices, ensuring faster processing and wider accessibility.

5. Integration with Object Detection:
Incorporating object detection can enhance system reliability by differentiating between valid gestures and background movements, minimizing false recognition during voting operations.

REFERENCES

1. M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini and C. Pahl, “Blockchain-based e-voting systems: A technology review,” Electronics, vol. 13, no. 1, p. 17, Dec. 2023.
2. A. Spinelli, “Managing elections under the COVID-19 pandemic: The Republic of Korea’s crucial test,” International Institute for Democracy and Electoral Assistance, Tech. Rep., 2020
3. D. Helbing, S. Mahajan, R. H. Fricker, A. Musso, C. I. Hausladen, C. Carissimo, D. Carpentras, E. Stockinger, J. A. Sanchez-Vaquerizo, J. C. Yang, M. C. Ballandies, M. Korecki, R. K. Dubey and E. Pournaras, “Democracy by design: Perspectives for digitally assisted, participatory upgrades of society,” Journal of Computational Science, vol. 71, Jul. 2023, Art. no. 102061.
4. S. Chambers and M. E. Warren, “Why deliberation and voting belong together,” Res Publica, vol. 31, no. 2, pp. 279–297, Jun. 2025.
5. U. Jafar, M. J. Ab Aziz, Z. Shukur and H. A. Hussain, “A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems,” Sensors, vol. 22, no. 19, p. 7585, Oct. 2022.
6. R. Joaquim, P. Ferreira and C. Ribeiro, “EVIV: An end-to-end verifiable internet voting system,” Computers & Security, vol. 32, pp. 170–191, Feb. 2013.
7. R. Taş and Ö. Ö. Tanrıöver, “A systematic review of challenges and opportunities of blockchain for e-voting,” Symmetry, vol. 12, no. 8, p. 1328, Aug. 2020.
8. C. D. González, D. F. Mena, A. M. Muñoz, O. Rojas and G. Sosa-Gómez, “Electronic voting system using an enterprise blockchain,” Applied Sciences, vol. 12, no. 2, p. 531,