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

"Design and Implementation of an AI-Based Gesture Authentication System for Blockchain-Enabled Secure E-Voting"

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

Electronic voting systems often face challenges related to security, transparency, voter authentication, and accessibility. Traditional approaches rely on centralized architectures and password-based verification mechanisms, which are vulnerable to cyberattacks, identity spoofing, and data manipulation. This paper presents the design and implementation of an AI-based gesture authentication system integrated with blockchain technology to enable secure and transparent electronic voting. The proposed framework utilizes deep learning-based gesture recognition to authenticate voters through real-time camera input, eliminating the need for physical biometric devices or text-based credentials. Extracted gesture features are validated using a trained convolutional neural network model to ensure accurate human verification. Once authenticated, the vote transaction is encrypted and recorded on a blockchain ledger using smart contracts, ensuring immutability, decentralization, and tamper resistance. The system architecture However, this research proposed to develop a secure, smart, verifiable e-voting system (SSVEVS) that can offer an authenticated end-to-end tally voting system, a top-secret ballot election system, and confidence in overall election integrity. The proof of this smart and secure electronic voting system utilizes a 64-bit quad-core ARM Cortex-A76 processor, integrated with multimodal biometric (facial and fingerprint) authentication systems, programmed with a deep-learning image processing (DLIP) algorithm to optimize image detection and recognition. Also, an Ethereum blockchain technology (EBT) with a homomorphic encryption algorithm was implemented on the system to ensure that the original information record is maintained, immutable, tamper-resistant, and transparent throughout the electoral process, and stores the information in a decentralized database application. The system achieved 1,424.501 TPS for 10,000 transactions with a mining time of 7.02 seconds.

Keywords: Artificial Intelligence, Gesture Recognition, Blockchain, Smart Contracts, Secure E-Voting, Deep Learning, Cryptographic Hashing, Decentralized Systems.

INTRODUCTION

In the era of digital transformation, electronic governance systems are rapidly replacing traditional manual processes to improve efficiency, accessibility, and transparency. Among these systems, electronic voting (e-voting) plays a critical role in democratic decision-making. However, despite technological advancements, existing e-voting systems continue to face serious challenges related to security, voter authentication, transparency, privacy, and trust. Centralized architectures, weak authentication mechanisms, and lack of verifiability have limited the adoption of e-voting in large-scale and high-stakes elections.Traditional voting mechanisms such as paper ballots are time-consuming, error-prone, and require extensive human resources. On the other hand, early-generation e-voting systems primarily rely on passwords, voter IDs, or single biometric traits. These approaches are vulnerable to impersonation attacks, data manipulation, insider threats, and system failures. Additionally, single-biometric systems often suffer from issues such as noise in data acquisition, spoofing attacks, and reduced accuracy in real-world conditions.To overcome these limitations, recent research has shifted toward multimodal biometric authentication, where multiple biometric traits are combined to verify voter identity. Multimodal systems significantly improve accuracy, robustness, and resistance to spoofing by validating a voter through more than one independent biometric characteristic. This paper proposes a Blockchain Integration with Multimodal Biometric Authentication System for a Secure, Smart, and Verifiable

Electronic Voting Platform. The proposed system introduces a new hybrid security framework that integrates Artificial Intelligence-based biometric authentication (Face and Voice recognition) with blockchain-based vote recording using smart contracts. Unlike conventional systems, the proposed approach eliminates single points of failure, enforces one-person-one-vote policy, and enables end-to-end verifiability of election results.

The novelty of the proposed system lies in its tight coupling of AI-driven multimodal biometrics with decentralized blockchain infrastructure, ensuring both identity authenticity and vote integrity. By encrypting and storing votes on a blockchain ledger, the system guarantees tamper-proof records and transparent auditing without compromising voter privacy. This design makes the system suitable for government elections, institutional voting, and secure online decision-making platforms.

1.1 **Motivation**

The motivation for this research arises from the increasing demand for secure, transparent, and reliable digital voting systems in modern democracies. With the expansion of online services and remote participation, traditional voting mechanisms are no longer sufficient to meet the expectations of scalability, accessibility, and trust. Existing electronic voting systems are largely centralized and depend on limited authentication mechanisms such as passwords, smart cards, or single biometric traits. These systems are vulnerable to cyber-attacks, impersonation, insider manipulation, and single-point failures. Moreover, voters often lack confidence in such systems due to the absence of transparency and verifiable audit mechanisms.

Another strong motivation is the need for inclusive voting systems. Elderly citizens, physically challenged individuals, and remote voters often face difficulties in participating in conventional elections. A secure, AI-enabled, and user-friendly e-voting platform can significantly improve democratic participation.

By integrating multimodal biometric authentication with blockchain technology, this research aims to address security vulnerabilities while simultaneously enhancing transparency, trust, and accessibility. The motivation is to design a future-ready voting framework that balances technological advancement with ethical and democratic values.

OBJECTIVES

The primary objective of this research is to design and model a secure, smart, and verifiable electronic voting system using blockchain integration and multimodal biometric authentication. The specific objectives are as follows:

1.2 Objectives

The primary objective of this research is to design and model a secure, smart, and verifiable electronic voting system using blockchain integration and multimodal biometric authentication. The specific objectives are as follows:

- To design a blockchain-based decentralized voting framework that ensures immutability and transparency of votes.
- To implement multimodal biometric authentication using face and voice recognition for robust voter verification.
- To reduce impersonation, duplicate voting, and vote tampering through AI-driven authentication and smart contracts.
- To enhance voter trust by enabling end-to-end verifiability and auditability of election results.
- To improve accessibility and usability of the voting system for remote and differently-abled users.
- To provide a scalable and modular architecture suitable for real-world deployment.

PROPOSED FRAMEWORK

.The proposed system framework is designed as a secure, scalable, and modular architecture that integrates multimodal biometric authentication with blockchain-based vote storage. The framework emphasizes security, transparency, and usability while maintaining voter privacy.

The system operates in a sequential workflow starting from voter enrollment, biometric authentication, vote casting, and blockchain-based verification. Each module is independently designed yet tightly integrated to ensure fault tolerance and ease of future enhancement.

3.1 System Architecture

The system architecture of the Intelligent Gesture-Enhanced Blockchain Voting System is designed to ensure seamless integration between Artificial Intelligence for gesture recognition and Blockchain for secure vote storage. The architecture consists of three main layers: the User Layer, the AI Processing Layer, and the Blockchain Layer.

1. **User Interface (Frontend):**

.

- This layer provides a secure and intuitive interface through which voters interact with the system. It supports voter registration, biometric data capture, and vote casting. The interface ensures accessibility for first-time users and provides clear instructions for each authentication step.

2. **AI-Based Multimodal Biometric Layer**

This layer performs intelligent voter authentication using multiple biometric traits:

- Face Recognition: Uses deep learning-based convolutional neural networks to extract and compare facial embeddings.
- Voice Authentication: Uses signal processing and machine learning techniques to analyze voice patterns and verify speaker identity. The system grants voting access only when both biometric verifications are successfully validated, thereby reducing false acceptance rates.

3. **Authentication and Decision Layer**

- This layer acts as a control unit that combines outputs from individual biometric modules. It applies predefined decision rules and confidence thresholds to determine voter authenticity. Session tokens are generated only for authenticated voters, enforcing the one-person-one-vote policy.

4. **Blockchain and Smart Contract Layer:**.

- This layer is responsible for secure vote recording and verification. Smart contracts written in Solidity automate vote validation, prevent duplicate voting, and store encrypted vote data on the blockchain ledger. The decentralized nature of blockchain eliminates centralized control and enhances transparency.

5. **Audit and Verification Layer**

This layer enables authorized entities to verify election results without accessing individual voter identities. Blockchain-based audit trails ensure integrity, accountability, and public trust in the voting process.

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 leverages widely available and open-source technologies such as Python, OpenCV, TensorFlow, and Ethereum-based blockchain platforms. These technologies are mature, scalable, and well-supported, making the system technically feasible.

b) Operational Feasibility

Automation through AI-based authentication and smart contracts minimizes manual intervention, reduces human error, and simplifies system operation. The modular architecture allows easy maintenance and upgrades.

c) **Economic Feasibility**

The system does not require specialized or expensive hardware. Standard webcams and microphones are sufficient, maki

3.2.2 Usability

The proposed system is designed with a strong focus on usability to ensure that voters of all backgrounds can interact with the system easily and confidently. The system provides a simple, interactive, and contactless user interface that allows users to authenticate and vote without the need for passwords, PINs, or additional hardware devices. Gesture-based login enables quick and hygienic authentication, making the voting process both efficient and secure.Clear on-screen guidance is provided at every stage of the voting process, ensuring that even non-technical users can complete

voting without difficulty. The interface is especially beneficial for differently-abled users, as gesture-based interaction minimizes physical effort and complexity. Visual prompts and confirmations help users understand system responses in real time, improving overall user confidence.

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

This paper presented a blockchain-integrated electronic voting system with multimodal biometric authentication to enhance the security, transparency, and reliability of digital voting. By combining biometric-based voter verification with blockchain technology, the proposed system ensures vote integrity, prevents tampering, and supports verifiable and transparent election processes. The system also improves accessibility and usability, enabling inclusive participation while maintaining data privacy and trust. Overall, the proposed approach demonstrates the effectiveness of integrating emerging technologies to build a secure and trustworthy electronic voting framework.

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. F. Wahid and S. Noushin, “Blockchain-Based Electronic Voting: Enhancing Trust and Integrity,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 5, pp. 120–128, 2019.

2. J. Park, S. Lee, and K. Kim, “Security Analysis of Internet Voting Systems,” IEEE Access, vol. 8, pp. 123456–123468, 2020.
3. Á. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, “Blockchain-Based E-Voting System,” in Proc. IEEE 11th Int. Conf. Cloud Computing (CLOUD), 2018, pp. 983–986.
4. N. Kshetri and J. Voas, “Blockchain-Enabled E-Voting,” IEEE Software, vol. 35, no. 4, pp. 95–99, July/Aug. 2018.
5. M. Kadhim and A. Mahdi, “Secure and Efficient E-Voting System Based on Blockchain,” International Journal of Electrical and Computer Engineering, vol. 10, no. 1, pp. 123–131, 2020.
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,