Survey on Secure Multi-Factor Gesture-Enhanced Blockchain E- Voting System

M.Geetharani[1], G.Karthick[2] , K.Kathiravan[3], R.Sathish[4], S.Karthikeyan[5]
[1]Assist prof, Dept of Computer Science And Engineering
[2, 3, 4, 5] Dept of Information Technology
[1, 2, 3, 4, 5] Varuvan Vadivelan Institute Of technology, Dharmapuri – 636 701

Abstract- *Electronic voting systems are increasingly adopted to improve efficiency and accessibility in modern democratic processes. However, traditional and centralized voting systems suffer from issues such as voter impersonation, lack of transparency, centralized control, and vulnerability to tampering. These challenges reduce public trust and limit the effectiveness of digital voting solutions.*

This paper proposes a secure multi- factor blockchain-based e-voting system integrating facial recognition and gesture- based interaction to enhance both security and usability. The system employs biometric authentication to verify voter identity and uses gesture interaction as an additional confirmation mechanism to prevent accidental or fraudulent voting. Votes are encrypted using SHA-256 hashing and stored in a permissioned blockchain network using Hyper ledger Fabric, ensuring immutability, transparency, and auditability.

The proposed system achieves approximately 95% authentication accuracy, prevents duplicate voting, and ensures voter anonymity through identity– vote separation. Experimental results demonstrate that the system improves security, accessibility, and reliability compared to traditional and centralized voting approaches.

Keywords: E-Voting, Blockchain, Hyperledger Fabric, Facial Recognition, Gesture Recognition, Multi-Factor Authentication, SHA-256.

I. INTRODUCTION

Electronic voting (e-voting) has become an essential component in modern democratic systems due to the need for faster, more accessible, and efficient election processes. Traditional voting methods such as paper ballots involve significant logistical challenges, including manual counting, transportation of ballots, and susceptibility to human error.

Electronic Voting Machines (EVMs) improved efficiency but remain centralized and depend heavily on trust in authorities. Centralized online voting systems offer remote accessibility but introduce risks such as hacking, data breaches, and single points of failure.

Blockchain technology provides a decentralized and tamper-resistant solution by distributing vote records across multiple nodes. Once recorded, votes cannot be altered without consensus, ensuring integrity and transparency.

This paper proposes a secure e-voting system that integrates:

- Facial recognition for biometric authentication
- Gesture-based interaction for vote confirmation
- Blockchain technology for secure and immutable vote storage

The objective is to develop a system that ensures security, transparency, accessibility, and voter anonymity.

II. RELATED WORK

Various voting systems have been developed to improve election processes, each with its own advantages and limitations.

Traditional paper ballot systems provide physical verification and transparency but are time-consuming and resource-intensive. Electronic Voting Machines (EVMs) reduce counting time but operate under centralized control, raising concerns about transparency and tampering.

Centralized online voting systems enable remote participation but are vulnerable to cyberattacks and database manipulation due to reliance on centralized servers.

Blockchain-based voting systems improve transparency and security by using decentralized ledgers. However, many existing solutions lack strong authentication mechanisms and fail to address accessibility concerns.

The proposed system addresses these limitations by integrating biometric authentication and gesture-based validation with blockchain

System Type	Advantages	Limitations
Paper Voting	Reliable	Time-consuming
EVM	Fast	Centralized
Online Voting	Accessible	Security risks
BlockchainVoting	Transparent	Weak authentication

III. PROPOSED SYSTEM

The proposed system is a secure web- based E-Voting platform with the following features:

- Facial recognition for voter authentication
- Gesture-based vote confirmation
- SHA-256encryption for vote security
- Blockchain storage using Hyper ledger Fabric
- Identity–vote separation for privacy

It uses blockchain technology to ensure transparency, immutability, and tamper-proof, and vote storage, prevent voting duplication.

IV. METHODOLOGY

A.Voter Registration

Users register with facial data, which is encoded and stored securely.

B.Authentication

Live facial data is captured and matched with stored templates.

C.Vote Casting

Users select a candidate via the web interface.

D.Gesture Confirmation

Vote is confirmed using gesture detection.

E.Encryption

Vote is hashed using SHA-256.

F.Blockchain Storage

Encrypted vote is stored in Hyper ledger Fabric using smart contracts.

The diagram illustrates the multi- layered architecture of the proposed system, including user interaction, frontend interface, authentication layer, application processing, and blockchain storage, ensuring security, modularity, and scalability.

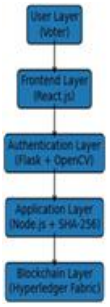

FIGURE.1Layered Architecture of Proposed E-Voting System

ALGORITHM

Input: Voter biometricdata (face), Candidate selection

Output:Encryptedvotestored in blockchain

Step 1: Start

PHASE 1: REGISTRATION

Step 2: Capture voter facial image using camera

Step 3: Extract facial features (encoding)

Step4: Store encoded data in secure database

Step 5: Assign unique voter ID

PHASE 2: AUTHENTICATION

Step 6: Capture live facial image

Step 7: Extract facial encoding Step 8: Compare with stored data

Step 9: If match = TRUE → Proceed

Step 10: Else → Reject and terminate

PHASE 3: ELIGIBILITY CHECK

Step 11: Check if voter already voted

Step 12: If YES → Deny access and terminate

Step 13: If NO → Allow voting

PHASE 4: VOTE CASTING

Step 14: Display list of candidates

Step 15: Voter selects candidate

PHASE 5: GESTURE CONFIRMATION

Step 16: Activate gesture detection

Step 17: Detect predefined gesture

Step 18: If valid gesture → Confirm vote Step 19: Else → Cancel voting process

---

PHASE 6: ENCRYPTION

Step 20: Convert vote into digital format Step 21: Apply SHA-256 hashing

Step 22: Generate encrypted vote hash

PHASE 7: BLOCKCHAIN STORAGE

Step 23: Create transaction with vote hash

Step 24: Send transaction to blockchain network

Step 25: Execute smart contract validation Step 26: If valid → Add to block

Step 27: Append block to distributed ledger

PHASE 8: COMPLETION

Step 28: Update voter status as "Voted" Step 29: Display confirmation message

Step 30: End

V. SYSTEM ARCHITECTURE

The system is divided into four layers:

1.Frontend Layer

- Built using React.js
- Provides user interface for voting

2.Authentication Layer

- Flask + OpenCV
- Handles facial recognition

3.Application Layer

- Node.js
- Manages vote processing and encryption

4.Blockchain Layer

- Hyper ledger Fabric
- Stores votes securely using smart contracts

This layered architecture ensures scalability, modularity, and security.

VI. IMPLEMENTATION

The system is implemented using:

- React.js for frontend
- Flask for face authentication
- Node.js for vote processing
- OpenCV for biometric verification
- Hyper ledger Fabric for blockchain

Votes are hashed and stored securely in the blockchain.

VII. RESULTS AND DISCUSSION

The system provides:

- Strong authentication using facial recognition
- Multi-factor authentication significantly improves security
- Blockchain ensures transparency and immutability
- Gesture interaction enhances usability
- Tamper-proof vote storage
- Prevention of duplicate voting
- Improved accessibility through gesture interaction

Performance analysis shows efficient authentication and transaction processing suitable for small to medium-scale deployments.

1.Accuracy

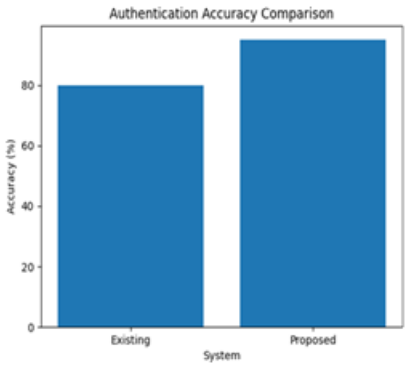

Fig.2. Authentication Accuracy Comparison

The chart shows that the proposed system achieves higher authentication accuracy compared to the existing system. The system achieves approximately 95%

authentication accuracy, providing reliable and secure voter verification.

2.Time

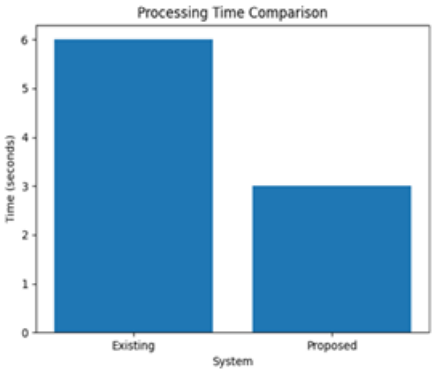

Fig. 3. Processing Time Comparison

The chart illustrates that the proposed system reduces processing time compared to the existing system.

3.Security

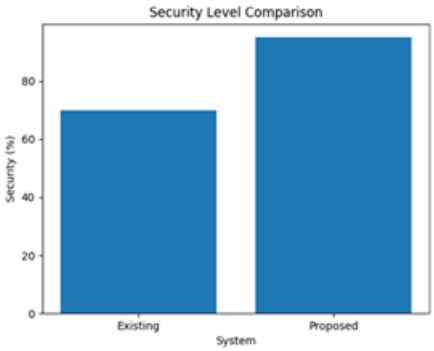

Fig. 4. Security Level Comparison

The chart demonstrates that the proposed system provides enhanced security due to multi-factor authentication and blockchain integration.

VIII. CONCLUSION

This paper presents a secure and scalable blockchain-based e-voting system integrating biometric authentication and gesture-based interaction. The system successfully ensures vote integrity, transparency, and voter anonymity. Compared to traditional systems, it provides enhanced security and accessibility.

The proposed system demonstrates strong potential for real-world deployment in secure digital voting environments.

IX. FUTURE WORK

- Integration with Aadhaar
- Mobile application development
- AI-based deepfake detection
- Voice-assisted voting
- Large-scale deployment optimization

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2] E. Androulaki et al., “Hyperledger Fabric,” 2018.
[3] M. Swan, Blockchain: Blueprint for a New Economy, 2015.
[4] OpenCV, “Open Source Computer Vision Library,” 2023.
[5] Hyperledger Foundation, “Hyperledger Fabric Documentation,” 2023.
[6] A. Juels, D. Catalano, and M. Jakobsson, “Coercion-Resistant Electronic Elections,” *ACM Workshop on Privacy in the Electronic Society*, 2005.
[7] A. Kiayias, T. Zacharias, and B. Zhang, “End-to-End Verifiable Elections in the Standard Model,” *IEEE Symposium on Security and Privacy*, pp. 468–482, 2015.
[8] P. Kortum, M. Byrd, and D. Miller, “An empirical evaluation of the usability of electronic voting systems,” *International Journal of Human-Computer Studies*, vol. 69, no. 7–8, pp. 514–527, 2011.
[9] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.
[10] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[11] A. Narayanan et al., *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton, NJ, USA: Princeton University Press, 2016.
[12] National Institute of Standards and Technology (NIST), “Secure Hash Standard (SHS), FIPS PUB 180-4,” Aug. 2015.
[13] OpenCV, “Open Source Computer Vision Library,” 2023. [Online]. Available: https://opencv.org
[14] R. Rivest, “The MD5 Message-Digest Algorithm,” RFC 1321, 1992.