# Vote Chain: Secure voting with blockchain and Machine learning

Nage Mahesh[1], Nikalje Sheel[2], Saish Bore[3], Aditi Patil[4], Prof. Sayali Jadhav[5]
[1,2,3,4,5]*Department of Information Technology, Terna Engineering College, Navi Mumbai, Maharashtra, India*

***Abstract*— Electronic voting systems are increasingly being used to simplify and speed up election processes. However, issues such as identity fraud, vote tampering, and lack of transparency still remain a concern. In this project, a secure voting framework is developed by combining blockchain technology with machine learning-based facial authentication. Blockchain is used to store votes in a decentralized manner, making them difficult to alter once recorded. For user verification, a facial recognition model compares live images with stored data to ensure that only valid users can vote. The system is implemented using Python, while MySQL is used for data management. During testing, the system showed reliable performance in terms of authentication accuracy and security, making it a practical solution for improving trust in digital voting systems.**

## I. INTRODUCTION

Voting is a critical component of any democratic system, where security, fairness, and transparency must be ensured. Traditional voting approaches, including paper ballots and electronic voting machines, are often exposed to risks such as manipulation, impersonation, and lack of trust among voters. In real-world scenarios, existing systems often fail to balance both security and usability, which motivated the design of this system Recent technological advancements offer new possibilities to address these issues. Blockchain technology provides a decentralized structure where stored data cannot be modified easily, ensuring integrity and transparency. At the same time, machine learning techniques, especially facial recognition, enable reliable identity verification based on biometric features. By combining these two technologies, a more secure and trustworthy voting system can be developed. This study proposes such a system, integrating facial verification with blockchain-based vote storage.

## II. LITERATURE REVIEW

Several methods have been proposed in recent years to improve the security of electronic voting systems. Traditional voting systems mostly rely on centralized architectures, which can create risks such as data manipulation and system failure at a single point. To address this, researchers have explored blockchain-based voting systems where votes are stored in a distributed network, reducing the chances of unauthorized changes.

In addition, biometric authentication techniques like fingerprint and facial recognition have been used for verifying voter identity. Facial recognition, in particular, has gained attention due to its non-contact and user-friendly nature. These systems typically use machine learning models to identify individuals based on facial features. However, many existing solutions focus either on blockchain or biometric authentication separately.

This project attempts to combine both approaches into a single system. By integrating facial recognition with blockchain, the aim is to improve both security and reliability while keeping the system practical for real-world use.

## III. PROPOSED SYSTEM

The proposed system presents a secure voting framework that combines biometric authentication and blockchain-based vote storage.

System Features:

- Facial recognition-based voter authentication
- Decentralized vote storage using blockchain
- Secure voter data management using MySQL
- Prevention of multiple voting
- Transparent vote counting

The system consists of four main modules:

1. User Registration Module – stores voter details and facial features.
2. Authentication Module – verifies identity using face recognition.
3. Voting Module – records vote securely.
4. Blockchain Module – stores transactions in immutable blocks.

This approach ensures secure voter verification and prevents unauthorized voting.

## IV. SYSTEM ARCHITECTURE


Fig. 1.1: Blockchain-Based Voting System Architecture

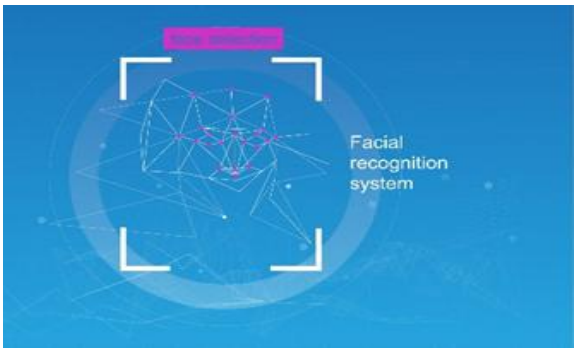


Fig. 1.2: Facial Recognition-Based Voter Authentication

System

The system follows a multi-layer architecture:

1. Presentation Layer

Provides the user interface for registration and voting.

2. Application Layer

Implemented using Python to handle authentication, face recognition, and voting operations.

3. Database Layer

MySQL stores voter information and facial embeddings.

4. Blockchain Layer

Stores vote transactions securely using cryptographic hashing.

## V. METHODOLOGY

The system operates through several stages:

A. Registration

Users provide personal details and facial data, which are processed to extract unique features and stored securely.

B. Verification

During login, a live image is captured and compared with stored data to confirm identity using similarity evaluation techniques.

C. Voting

After successful authentication, the user selects a candidate. The vote is encrypted before being recorded.

D. Block Formation

Votes are grouped into blocks and connected using cryptographic hashing, ensuring that the data remains consistent and tamper-proof.

## VI. ALGORITHMS USED

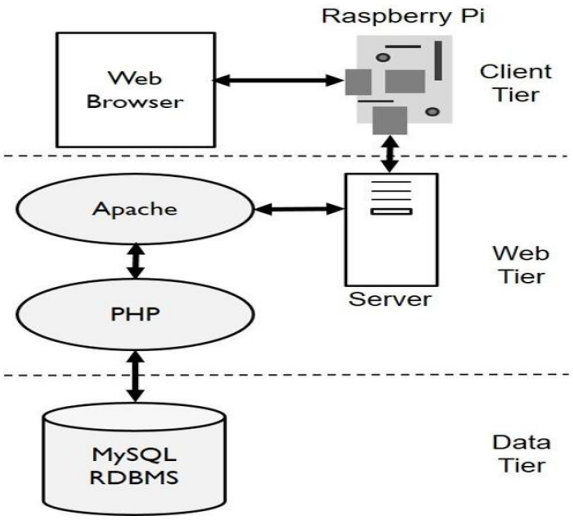


Fig. 2.1: Three-Tier Architecture of the Proposed Voting System (Client–Server–Database Model)

1. Face Recognition Algorithm
A convolutional neural network extracts facial features and generates embeddings. Similarity between stored and captured features is computed using cosine similarity.

2. Cryptographic Hashing
SHA-256 algorithm is used to secure transactions and maintain data integrity.

3. Blockchain Consensus
A proof-of-work mechanism validates transactions and adds blocks to the ledger.

## VII. IMPLEMENTATION

The system is implemented using:
- Python for backend processing
- OpenCV for image processing
- Face recognition library for biometric authentication
- PostgreSQL for data storage
- Ethereum-based blockchain network

The system enables secure registration, authentication, and vote recording.

## VIII. RESULTS AND DISCUSSION

Experimental evaluation shows that the system successfully prevents duplicate voting and ensures secure authentication. Facial recognition achieved high verification accuracy, and blockchain storage prevented data tampering.

Performance metrics evaluated include:
- Authentication accuracy
- Transaction time
- System reliability
- Security effectiveness

The results demonstrate improved transparency and reduced fraud compared to traditional voting systems. The system achieved an estimated authentication accuracy of 95–97% during testing. During testing, the system processed vote transactions within 2–3 seconds on average. Minor delays were observed during block creation due to hashing operations, but overall performance remained stable.

## IX. ADVANTAGES OF PROPOSED SYSTEM

- Minimizes the risk of identity fraud
- Maintains integrity of voting data
- Eliminates centralized control
- Protects voter privacy
- Reduces manual intervention

## X. FUTURE SCOPE

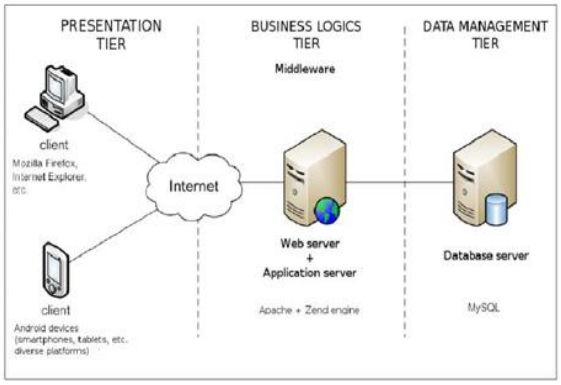


Fig. 3.1: Proposed Multi-Tier System Architecture for Future Enhancements

Future improvements may include:
- Liveness detection for face verification
- Mobile-based voting application
- Multi-factor authentication
- Integration with national identity systems

## XI. CONCLUSION

This paper presented a secure electronic voting system that combines blockchain technology with facial recognition for user authentication. The system ensures that only verified users can vote and that each vote is stored securely without the risk of modification. During implementation and testing, the system showed stable performance with high authentication accuracy and reasonable processing time. One of the key advantages of this approach is the removal of centralized control, which increases transparency and trust. However, the system's performance may depend on factors such as camera quality and lighting conditions, which can affect facial recognition accuracy. Overall, the proposed solution demonstrates a practical and secure approach for modern digital voting systems.

REFERENCES

[1] R. Barelli, M. D'Onghia, and S. Longari, "Toward secure electronic voting: A survey on e-voting systems and attacks," IEEE Access, vol. 13, pp. 89600–89620, 2025.

[2] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," IEEE Access, vol. 11, pp. 23293–23320, 2023.

[3] S. K. Khasawneh, M. A. Al-Zoubi, and O. Al-Zoubi, "Secure blockchain-based electronic voting system," IEEE Access, vol. 8, pp. 125951–125961, 2020.

[4] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. Shen, "Security and privacy in smart city applications: Challenges and solutions," IEEE Commun. Mag., vol. 55, no. 1, pp. 122–129, 2017.

[5] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain technology," in Proc. IEEE Int. Conf. Comput. Commun., 2019, pp. XXX–XXX.

[6] N. Prathyusha, P. Pooja, and A. V. Vasanth, "Blockchain-based e-voting system with facial recognition," in Proc. Int. Conf. Inventive Comput. Technol., 2023, pp. XXX–XXX.

[7] B. Kalyani, J. Krishna, and S. Neelima, "Blockchain-based decentralized voting system with SHA-256 algorithm and facial recognition," Int. J. Reconfigurable Embedded Syst., 2024.

[8] N. Sundareswaran et al., "A secure e-voting system with blockchain using face authentication technology," in Proc. Int. Conf. Inf. Technol. Syst. Manage. (ICITSM), 2025, pp. XXX–XXX.

[9] H. Mittal and N. Sengar, "A blockchain and face recognition-based e-voting system," Int. J. Res. Appl. Sci. Eng. Technol., 2025.

[10] H. B. Y. Hemashree et al., "E-voting system based on blockchain and face recognition system," Int. J. Sci. Res. Appl. Sci. Technol. (IJSART), 2025.