

A SECURE BLOCKCHAIN-BASED SMART VOTING SYSTEM WITH DUAL BIOMETRIC AUTHENTICATION USING FACIAL RECOGNITION AND FINGERPRINT SIMILARITY VERIFICATION

Mrs.M.Kalaimani ,M.E.,^[1], M.Nisma^[2], H.Hasbiya^[3], T.Harinisri^[4] ^[1]Assistant Professor , ^[2], ^[3], ^[4] UG Student

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING ARASU ENGINEERING COLLEGE ,
KUMBAKONAM

Abstract: The need for safe, transparent, and trustworthy election procedures has grown due to the quick expansion of digital voting systems. In order to guarantee voter legitimacy, this proposed system integrates real-time facial verification using the Grassmann algorithm and fingerprint image authentication with a blockchain-based electronic voting framework. Votes are stored as immutable transactions using blockchain technology, where each vote that is successfully cast is mined and added as a new block using cryptographic hashing methods like SHA-256. Through a secure image upload process, voters must register their fingerprint samples and facial images, which are encrypted and connected to their individual blockchain voter identification number. In order to precisely match the live captured face with the registered data, real-time facial recognition is carried out during the voting process using the Grassmann manifold-based similarity measurement. Fingerprint verification concurrently uses a structured similarity check flow that includes pattern matching against stored biometric templates, image preprocessing, ridge enhancement, and minutiae feature extraction. In order to assess authentication validity and guarantee accurate identity confirmation, the similarity score is calculated. In addition to preventing unauthorized access, impersonation, and duplicate voting attempts, the combined biometric similarity check mechanism greatly increases accuracy. Through dual biometric validation and unique voter ID mapping, the one-person, one-vote principle is rigorously upheld. The blockchain can dynamically adapt to the voting workload while preserving data integrity and consensus thanks to the block sealing concept. The blockchain network safely gathers and maintains all voting records, guaranteeing transparency, auditability, and resistance to manipulation. By combining cutting-edge biometric authentication with decentralized ledger technology, the suggested framework greatly increases election security, reduces electoral fraud, and boosts public confidence in electronic voting systems.

Keywords: permissioned Proof of Authority (PoA) blockchain, smart contracts, SHA-256 hashing, blockchain voting, dual biometric authentication, Grassmann manifold, facial recognition, fingerprint minutiae matching, minutiae feature extraction, offline polling, booth-level security, cryptographic device_pairing.

Introduction : Election accessibility and efficiency are being enhanced by the growing use of electronic voting systems. They lessen the amount of manual labor needed in conventional paper-based voting systems and

enable quicker vote counting.

However, voter impersonation, ballot tampering, and database manipulation are some of the security issues that digital voting systems must deal with

Conventional voting techniques are dependable, but they are slow and vulnerable to human error when counting votes. Election integrity was a concern because early electronic voting systems frequently lacked adequate security measures and transparency. As a result, a secure voting system that guarantees voter authentication, stops duplicate voting, and offers an open method of recording votes is required.

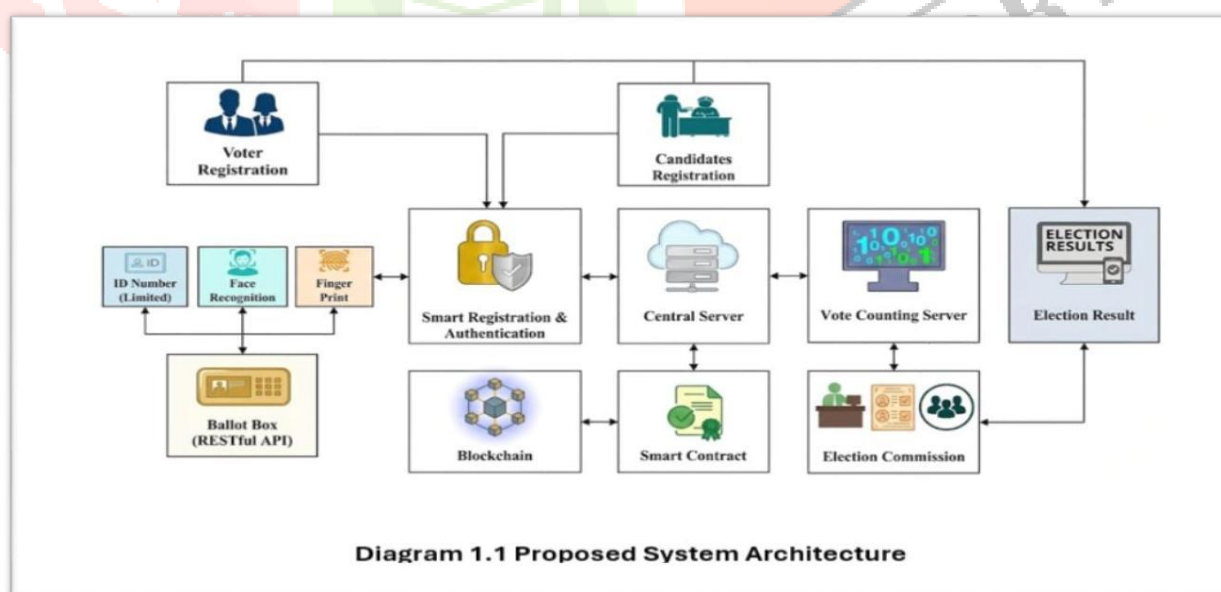
In order to confirm voter identity, this paper suggests a blockchain-based electronic voting system that employs dual biometric authentication. To guarantee that only eligible voters can cast ballots, the system combines fingerprint verification with facial recognition. Votes are safely stored as immutable transactions using blockchain technology, guaranteeing transparency and guarding against manipulation.

Using a laptop as the voting terminal and a mobile device for biometric collection, a prototype system was created. Voter registration, biometric verification, voting, and blockchain storage are all included in the system. The suggested method enhances electronic voting systems' security, openness, confidence.

To increase election efficiency, a number of electronic voting systems have been created. Although they increased counting speed, traditional electronic voting machines lacked auditability and transparency. Because blockchain technology offers decentralized and impenetrable data storage, it has recently been investigated as a potential solution to these problems.

Mobile applications and digital identity verification are used by some blockchain-based voting systems, like **Voatz** and **Votem**. However, these systems may still be vulnerable to security issues like device attacks or inadequate authentication methods because they frequently rely significantly on internet connectivity.

Secure identity systems frequently employ biometric authentication techniques like facial and fingerprint recognition. While facial recognition examines facial features to confirm identity, fingerprint recognition relies on identifying distinct ridge patterns and minute points. Combining several biometric techniques lowers the possibility of impersonation and increases authentication system and accuracy.



Despite these advancements, a lot of systems still rely on cloud-based infrastructure or a single biometric technique. By combining dual biometrics with blockchain and supporting offline voting environments, the suggested system enhances current methods and is better suited for actual polling places.

2. System Architecture

A prototype implementation and a real-world deployment model are supported by the modular architecture of the suggested voting system. The architecture is made to be scalable for big elections while guaranteeing safe voter authentication, dependable vote recording, and simple monitoring.

2.1 Voter Registration

Voters submit personal information, fingerprint samples, and photos of their faces during the registration process. A database connected to the voter's distinct ID processes and safely stores these biometric characteristics..

2.2 Biometric Authentication

The system conducts real-time biometric verification when a voter shows up at the polling place.

- **Facial Recognition:** The Grassmann Manifold similarity measurement is used to compare the captured facial image with the stored template
- **Fingerprint Verification:** Images of fingerprints are processed to extract minute details, which are then compared to pre-stored fingerprint templates.

Both authentication methods must be successful before allowing the voter to proceed.

2.3 Interface for Voting

The voter can choose a candidate via a graphical user interface after authenticating. A NOTA option is also included in the system.

2.4 Vote Storage on Blockchain

SHA-256 hashing is used to transform each vote into a secure transaction. After that, the vote is kept in a private blockchain network as a block. This guarantees that the vote cannot be changed or removed once it has been recorded.

2.5 Administrative Surveillance

Vote totals and system status are shown in real time on an admin dashboard. This preserves voter privacy while enabling election authorities to keep an eye on voting activity.

2.6 Deployment of Prototypes

The Tkinter interface, SQLite database, biometric processing modules, and blockchain simulator are all run on a Windows laptop (Intel i5+, 8GB RAM) that serves as the central voting terminal for the prototype system. For biometric collection, an Android smartphone equipped with a camera and fingerprint sensor is connected via ADB for safe data transfer. While encrypted transactions are momentarily stored using AES-256 prior to synchronization with the blockchain, booth identities are created using SHA-256 hashed hardware identifiers.

2.7 Deployment of Production

The system is deployed in the real world as a secure voting kiosk that incorporates a touchscreen interface, fingerprint scanners, and facial recognition cameras. A hardened operating system and an ARM-based processor with a TPM security module power the system.

Votes are stored in a permissioned blockchain via Proof-of-Authority (PoA) consensus, dual biometric authentication, candidate selection, and SHA-256 transaction hashing. [Table 1.2]

3. Methodology

The planned electronic voting system's operation is described in this section. To provide a safe and transparent voting process, the system handles voter registration, biometric verification, vote casting, and blockchain storage.

3.1 Booth Initialization

The voting device is started and securely configured prior to the start of voting. Using system information like MAC address and device ID, each booth device creates a distinct hardware identity. To generate a secure device fingerprint, this data is hashed using the SHA-256 technique.

In order to save voter data, biometric templates, and voting status, the system also initializes the local database. Vote transactions can be recorded via the blockchain module. Voter Registration

The voter supplies personal information, including name and voter ID. The system also

While fingerprint images are enhanced to identify minute details like ridge endings and bifurcations, facial images are processed to extract distinctive facial features. These biometric characteristics are connected to the voter's ID and safely stored in the database. To preserve voter privacy, the stored data is encrypted.

3.2 Dual Biometric Authentication

The system verifies a voter's identity in real time when they get to the polling place.

First, a similarity measurement method is used to compare the voter's face with the stored facial template after it has been captured by the camera. The system then extracts minute details from the voter's fingerprint to compare with the registered fingerprint template.

Only after facial recognition and fingerprint verification are successful can the voter cast their ballot. In addition to enhancing security, this dual authentication stops impersonation.

3.3 Vote Casting

- After successful authentication, the voting interface displays the list of candidates along with their symbols

Phase	Prototype Tools	Production Augments	Latency Target
Reg	ADB stream	IR depth cam	<10s
Auth	<u>face recog</u> + Gabor	Jetson AI accel	<300ms
Vote	<u>Tkinter</u>	Haptic LED touch	<0.5s
Chain	Local sim	<u>PoA</u> cluster	<2s/block

Table 1.1. System Development Phases and Performance Latency Targets

and a NOTA (None of the Above)

captures the voter's facial image and fingerprint sample using the biometric devices.

option. The voter selects their preferred candidate using the graphical interface.

- The graphical user interface is used by the voter to choose their favorite candidate.
- The system creates a vote record with the voter ID, chosen candidate, timestamp, and booth ID after the vote is verified.

3.4 Blockchain Vote Storage

- The SHA-256 hashing is used to transform the vote record into a secure transaction. The blockchain network then adds the hashed transaction to a block.
- Once the vote is recorded, it cannot be changed thanks to the blockchain. In order to avoid duplicate voting, the voter's status in the database is also updated to "Voted."

4. Experimental Evaluation and Results

The Simulated voters were used to test the prototype system in order to assess system performance and authentication accuracy.

While preventing unwanted access, the dual biometric authentication achieved high accuracy in confirming eligible voters. While fingerprint verification successfully matched stored templates, facial recognition performed consistently in a variety of lighting and viewing angles.

By verifying the voter status, the system was able to successfully stop duplicate

voting attempts. prior to permitting a vote. Vote records were kept safe and unchangeable thanks to blockchain storage. Performance tests demonstrated the system's speedy vote processing, with authentication and vote recording typically taking less than a second.

5. Results and Discussion

The findings demonstrate that the security of electronic voting systems is greatly increased when blockchain technology is combined with dual biometric authentication. Blockchain guarantees that vote records cannot be changed, and the use of facial recognition and fingerprint verification lowers the possibility of voter impersonation.

Additionally, the system's offline-capable design makes it appropriate for polling places with spotty internet access. The suggested system offers greater auditability and transparency than conventional electronic voting machines.

Large-scale deployment, however, might call for more infrastructure and more testing using bigger datasets. Stronger cryptography techniques and improved biometric sensors are possible future developments.

6. Conclusion and Future Work

In this paper, a secure electronic voting system utilizing dual biometric authentication—facial recognition and fingerprint verification—and blockchain technology was presented.

Aspect	Prototype (Laptop + Mobile)	Production (Auth System + LED Touch)
Input	USB-A/B mobile camera/sensor	Integrated IR camera + optical scanner
Display	Laptop screen/keyboard	19" LED capacitive touchscreen
Portability	High (demo-ready)	Fixed booth kiosk, ruggedized
Latency	<0.5s (consumer HW)	<0.3s (edge AI optimized)
Security	Software pairing	Hardware TPM + physical seals

Table 1.2. Prototype vs Production Hardware Architecture of the Blockchain-Based Voting System

Votes are stored in an unchangeable blockchain ledger, secure voter identification is guaranteed, and duplicate voting is prevented.

High authentication accuracy and effective vote processing were shown by the prototype implementation. The suggested system improves the security and transparency of electronic voting systems by combining biometric authentication with decentralized data storage.

Future research will concentrate on enhancing scalability, incorporating cutting-edge cryptographic methods, and evaluating the system in extensive election settings.

7. Reference

- [1] Hamza Baniata and Giovanni Caluna, "BP-Vot: Blockchain-Based e-Voting Using Smart Contracts, Differential Privacy, and Self-Sovereign Identities," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3548404.
- [2] Mosbah Alown, Mehmet Sabir Kiraz, and others, "Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3531349.
- [3] M. S. Muncshwara, V. Vijayakumar Kallur, A. S. Chethan, Vaishnavi, M. Giridhar Rao, and S. R. Rao, "E-Vote 2.0: Strengthening Democracy Through Dual Blockchain Technology," in *Proc. IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, 2025.
- [4] K. V. Dedeepya, K. Medini, A. D. Annapurna, and S. S. Shashank, "A Scalable and Secure Smart Voting Framework Using Dual-Storage, Blockchain Ledger, and Facial Recognition for Tamper-Proof Biometric Authentication," in *Proc. International Conference on Communication,*

Computer, and Information Technology (IC3IT), 2025.

- [5] V. P. Menon, A. S. Tharshith, P. Aryan, K. S. Pande, and S. Kamatchi, "Blockchain-Based Framework for Secure and Transparent E-Voting Using Ethereum: An Alternative to Traditional EVMs," in *Proc. IEEE International Conference on Contemporary Computing and Communications (InC4)*, 2025.