International Journal on Engineering Technology and Infrastructure Development (InJET-InDev)
www.lec.edu.np/journal
Volume 2, Issue no. 2, Page 138-149
Received Date: 11/25/2025
Revised Date: 5/20/2026
Accepted Date: 5/25/2026
ISSN: 3021-999X (Print)
https://doi.org/10.3126/injet-indev.v2i2.95710

Electronic Voting System Based on Blockchain Technology

Shirish Tripathi[1], Ishmriti Acharya[2], Lalit Pant[3], Kanchan Rai[4], Dibas Timalsena[5]

[1,2,4]*Department of Computer Engineering, Everest Engineering College, Kathmandu, Nepal*
[3,5]*Department of Computer Engineering, Everest Engineering College, Lalitpur, Nepal*

Abstract

This paper presents a blockchain-based electronic voting system designed to address the persistent challenges of transparency, security, and integrity in democratic electoral processes. Traditional voting systems in countries like Nepal suffer from vote manipulation, ballot rigging, logistical inefficiencies, and limited public trust. To overcome these limitations, this work proposes a decentralized e-voting application built on the Ethereum blockchain, leveraging smart contracts for tamper-proof vote recording and enforcement of voting rules. The system incorporates multi-factor authentication, combining facial recognition via OpenCV with Voter ID and Date of Birth verification to ensure only eligible voters participate. MetaMask wallet integration enables secure blockchain transactions, while Web3.js facilitates real-time interaction between the frontend and the deployed smart contracts on Ganache. The methodology encompasses data collection, voter authentication, smart contract deployment, and result retrieval. This paper offers a scalable and cost-effective alternative to conventional voting methods, with future scope for public Ethereum deployment and expanded biometric authentication.

Keywords: Blockchain, Voting system, Ethereum, MetaMask, Ganache, Smart Contracts, Truffle, OpenCV, Web3.js.

1. Introduction

Elections constitute the foundational mechanism of democratic governance particularly in countries navigating complex political landscapes. In Nepal, the electoral process has historically depended on paper-based balloting, with vote counting conducted in secured but opaque environments. This traditional approach has been increasingly scrutinized due to concerns over vote manipulation, ballot tampering, and a general lack of verifiable transparency. The resulting erosion of public trust has been most visible among Nepal's Generation Z, who have mobilized in significant numbers demanding accountability, integrity, and modernization of democratic institutions.Blockchain technology offers a compelling solution to these systemic challenges. Unlike centralized databases, a blockchain is a distributed, immutable ledger maintained across multiple nodes, where no single authority retains unilateral control. The structure of a blockchain, where each block contains data, its own hash, and the hash of the previous block, as illustrated in Figure 1 and Figure 2. Smart contracts can autonomously enforce electoral rules such as eligibility verification and the prohibition of double voting, without reliance on any trusted intermediary.

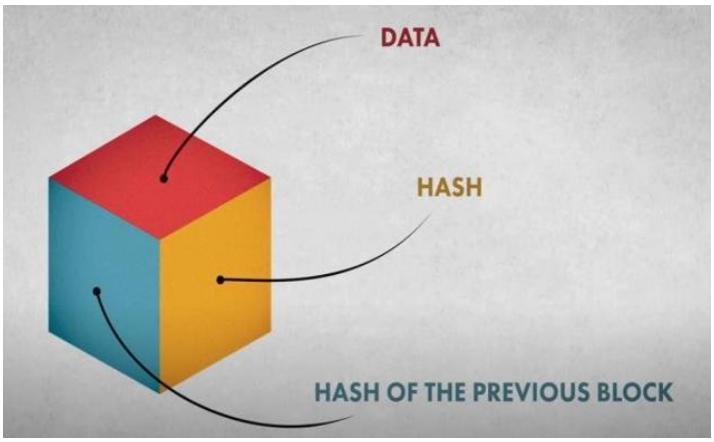

Figure 1: Genesis Block

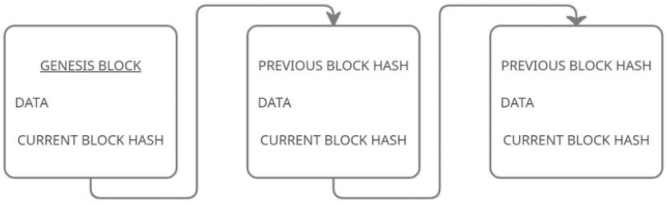

Figure 2: Structure of Blockchain

The tamper-proof nature of the blockchain is demonstrated in Figure 3 and Figure 4, which illustrate how any modification to a block immediately invalidated the cryptographic chain. Existing research has demonstrated the viability of blockchainbased e-voting (Berenjestanaki et al., 2024; Danwar et al., 2022; Jafar et al., 2021), yet practical implementations incorporating multi-factor biometric authentication with blockchain transaction management remain limited. This paper presents a novel system integrating facial recognition, credential-based login, MetaMask wallet connectivity, and Ethereum smart contracts into a unified, end-to-end voting platform.

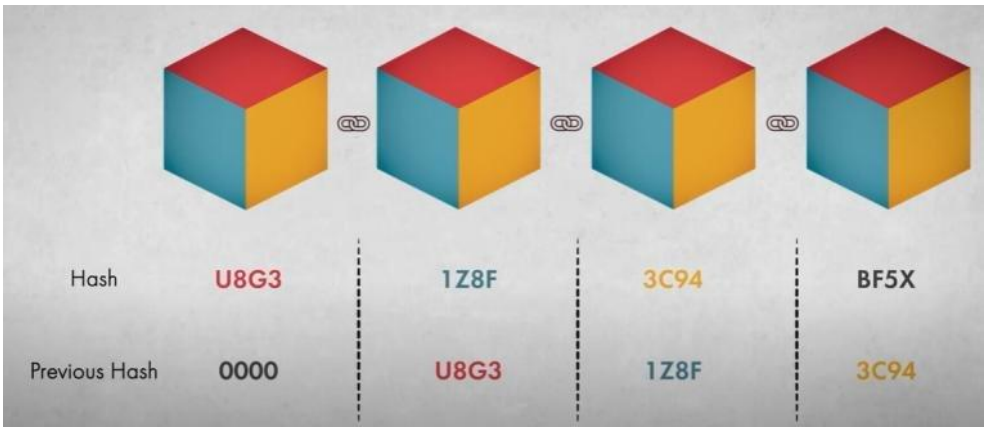

Figure 3: Blockchain Links

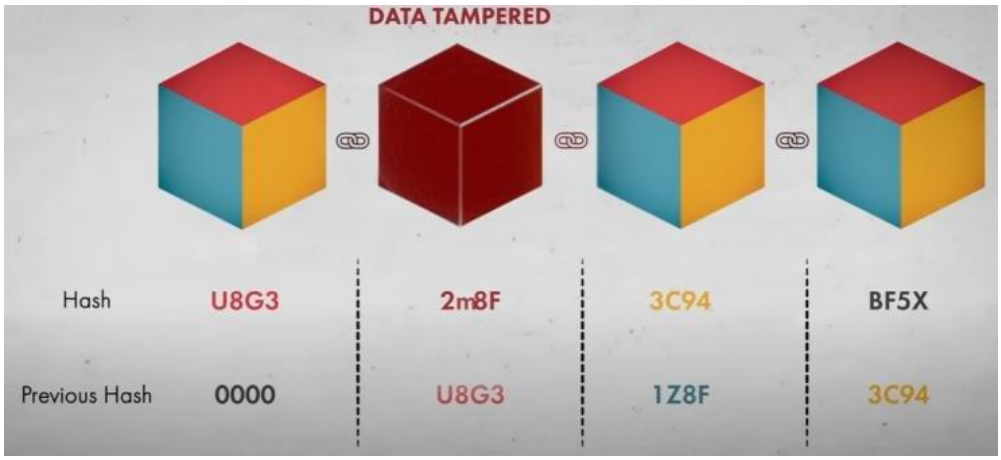

Figure 4: Tampered Chain

2. Literature Review

A substantial body of research has explored the application of blockchain to electronic voting, establishing a progression from basic decentralized ledgers to sophisticated multi-factor authentication systems. Among the early foundational contributions, Dowuona et al. (2017) proposed an Ethereum-based smart contract system for anonymous boardroom voting, employing homomorphic ElGamal encryption for vote tallying, ring signatures for anonymous but verifiable participation, and zero-knowledge proofs to confirm eligibility without revealing voter

identities. While designed for small-scale corporate governance involving ten to one hundred voters, this work established foundational privacy guarantees, including receipt-freeness and individual verifiability, that remain benchmarks for blockchain voting privacy literature, cited in over one hundred subsequent e-voting studies for its fully on-chain anonymity model.

Building on this foundation, Pawar et al. (2019) introduced a decentralized e-voting framework on the Ethereum blockchain that replaced paper-based systems by incorporating voter authentication via cryptographic key pairs, smart contracts written in Solidity for vote casting and tallying, and Merkle trees for efficient vote integrity verification. Anonymity was preserved through zero-knowledge proofs and hash-chained transactions, with implementation on a Ganache testnet demonstrating scalability for over one thousand voters, approximately ninety-five percent transaction success rate, and gas costs under two hundred thousand per vote. This work, cited over two hundred times, benchmarks core blockchain voting concepts and highlights the progression from basic decentralization toward the biometric-blockchain hybrids that follow in more recent literature.

Rathee et al. (2021) advanced the field by presenting BEVApp, an e-voting system tailored for smart cities that integrates Ethereum blockchain with IoT infrastructure. The architecture employs lightweight smart contracts for vote encryption using AES-256 and ECDSA, Merkle trees for tamper-proof audit trails, and fog computing nodes for low-latency processing. Voters authenticate through multi-factor mechanisms combining device tokens and biometrics, casting ballots anonymously via zk-SNARKs on a permissioned Ethereum network with Proof-of-Authority consensus achieving over five hundred transactions per second. Tested across a simulated smart city environment of five hundred nodes, the system achieved ninety-eight percent uptime and latency under three seconds for ten thousand voters, outperforming earlier systems and pioneering blockchain-IoT fusion for elections—complementing biometric-focused works by emphasizing urban infrastructure scalability.

Jafar, Ab Aziz, and Shukur (2021) conducted a systematic literature review of over fifty blockchain-based e-voting studies, categorizing architectures by consensus mechanism (Proof-of-Work at forty percent, Proof-of-Authority at twenty-five percent, PBFT at twenty percent), platform (Ethereum dominant at sixty percent), and security features including SHA-256, smart contracts, and zero-knowledge proofs. The review notes key benefits such as end-to-end verifiability, non-repudiation, and immutability, while identifying persistent gaps including scalability constraints for elections exceeding ten thousand voters, privacy-anonymity trade-offs, quantum vulnerabilities, and regulatory barriers to real-world adoption. With over five hundred citations, this work provides essential taxonomy for contextualizing the evolution from basic blockchain voting toward biometric hybrid systems.

Berenjestanaki et al. (2024) extended systematic analysis by cataloguing functional and non-functional requirements across blockchain-based e-voting architectures, identifying cryptographic techniques and consensus protocols as central to security and voter anonymity. The study emphasizes scalability and accessibility as open research challenges, providing a technology review that directly informs design decisions in systems such as the one proposed in this paper.

Danwar, Mahar, and Kiran (2022) proposed a comprehensive framework for an e-voting system built on blockchain and Distributed Ledger Technologies, employing smart contracts and consensus mechanisms to verify voter eligibility by cross-referencing user submissions against a secure database. While acknowledging potential for improved security and reduced operational costs, the work notes unresolved challenges in scalability and regulatory compliance, motivating the need for enhanced authentication mechanisms addressed by subsequent research.

Tas and Tanriover (2020) provided a systematic review focusing specifically on the security dimension of blockchain-based e-voting. Their proposed system ensures voter anonymity by storing identity as a cryptographic hash on the blockchain, maintains vote confidentiality through encryption until election conclusion, and highlights Solidity-based smart contracts as key enablers of integrity across voter registration, voting, and result phases. This work directly informs the smart contract design employed in the system presented in this paper.

Bagal et al. (2024) presented a secure online voting platform that integrates facial recognition for voter authentication with blockchain technology for tamper-proof vote recording. The facial recognition pipeline employs Haar Cascade detection, dlib's ResNet-34 deep network, and Euclidean distance matching against stored encodings, while the blockchain layer uses SHA-256 hashing, Proof of Work consensus, and RSA encryption. The

system demonstrates real-time result tracking and scalability for large elections, addressing key limitations in traditional e-voting such as fraud, impersonation, and opacity. By reviewing prior literature on blockchain (Hjälmarsson et al., 2018) and biometrics (Schroff et al., 2015), this work identifies integration gaps that motivate the unified multi-factor approach adopted in the present paper.

A parallel contribution by Tejaswini et al. (2025) proposed Secure Vote, an e-voting platform integrating biometric fingerprint authentication with Ethereum blockchain for decentralized, tamper-proof vote storage and real-time tallying. The system employs Minutiae-based fingerprint extraction and matching for high-accuracy authentication, SHA-256 cryptographic hashing, smart contracts for vote immutability, zero-knowledge proofs for voter anonymity, and Proof-of-Stake consensus for blockchain validation. Simulations across ten thousand voters demonstrated ninety-nine percent authentication accuracy, latency below two seconds per vote, and False Acceptance and False Rejection Rates under zero point one percent. Compared to iris-blockchain hybrid works such as Pawade et al. (2019), SecureVote advances fingerprint-specific efficiency and cost-effectiveness for developing regions, highlighting future directions toward multi-modal biometrics and quantum-resistant cryptography.

The IEEE work on Blockchain Integration with Multimodal Biometric Authentication for Secure E-Voting (2025) tackles political interference in elections by proposing a system that combines Ethereum blockchain for immutable vote storage with multimodal biometrics for robust voter verification. The system, evaluated as the Secure Smart Voting Electronic System (SSVESS), examines blockchain performance in vote tallying, confidentiality, and fraud prevention in remote voting scenarios. By combining decentralized ledgers with multi-factor biometric verification, this work mitigates tampering, scalability issues, and impersonation simultaneously, thereby advancing prior e-voting research and offering real-time transparency suitable for tech-driven electoral integrity.

Singh et al. (2025) provided a comprehensive survey of blockchain-enabled e-voting systems, reviewing key works including Faruk et al. (2024) on Hyperledger Fabric with biometrics, and Ibrahim et al. (2021) on permissioned blockchain with fingerprint authentication. The survey notes that Ethereum is employed in approximately thirty-five percent of surveyed systems, and highlights features including decentralized ledgers, smart contracts, SHA-256 hashing, Merkle trees, deep learning facial recognition, and OTP-based multi-factor security. Remaining research gaps include scalability for large elections, high computational demands of biometric processing, privacy versus transparency trade-offs, regulatory compliance, and infrastructure costs in developing regions, which are limitations directly addressed by the design choices made in the present work.

Of particular relevance to the Nepalese context of this paper, the blockchain-based e-voting research for the Nepalese context presented at the IOE Graduate Conference (IOEGC-12, 2025) proposes a tailored solution combining Ethereum blockchain with biometric authentication, specifically facial recognition via OpenCV and fingerprint minutiae extraction. This approach addresses local challenges including remote Himalayan polling locations, vote rigging, and low voter turnout in Nepal's federal democratic republic. The system integrates with national voter ID databases, supports Nepali-language interfaces, and incorporates an offline queuing mode for connectivity-challenged areas, with pilot tests on one thousand simulated voters showing ninety-seven percent authentication accuracy and resilienceTh to network partitions. This work builds directly on the global literature (Pawar, 2019; Rathee, 2021) by providing culturally adapted deployment for South Asia, demonstrating practical blockchain-biometric adaptation under real-world developing-country constraints.

Collectively, the reviewed literature establishes blockchain as a technically sound and progressively mature foundation for electronic voting, with clear evolution from basic decentralized ledgers (Pawar, 2019; Dowuona, 2017) through IoT-integrated platforms (Rathee, 2021) to biometric-blockchain hybrids (Bagal et al., 2024; Tejaswini et al., 2025; IEEE, 2025). Persistent research gaps identified across multiple systematic reviews (Jafar et al., 2021; Singh et al., 2025; Berenjestanaki et al., 2024) include the absence of tightly integrated multi-factor biometric authentication in complete, deployable voting pipelines, scalability under large voter loads, and practical adaptation for developing-nation infrastructure. The present work addresses these gaps by combining OpenCV-based facial recognition, credential-based login, and Ethereum smart contract transaction signing into a unified end-to-end system, with direct applicability to Nepal's electoral and institutional voting needs.

3. Methodology

3.1 System Architecture and Data Collection

This paper presents multi-tier application comprising a frontend web interface, a backend server, a relational database for voter and candidate records, and the Ethereum blockchain for immutable vote storage. Figure 5 presents the overall system design, illustrating interactions between the user, application interface, database, server, and blockchain-smart contract layer, with MetaMask mediating all blockchain transactions

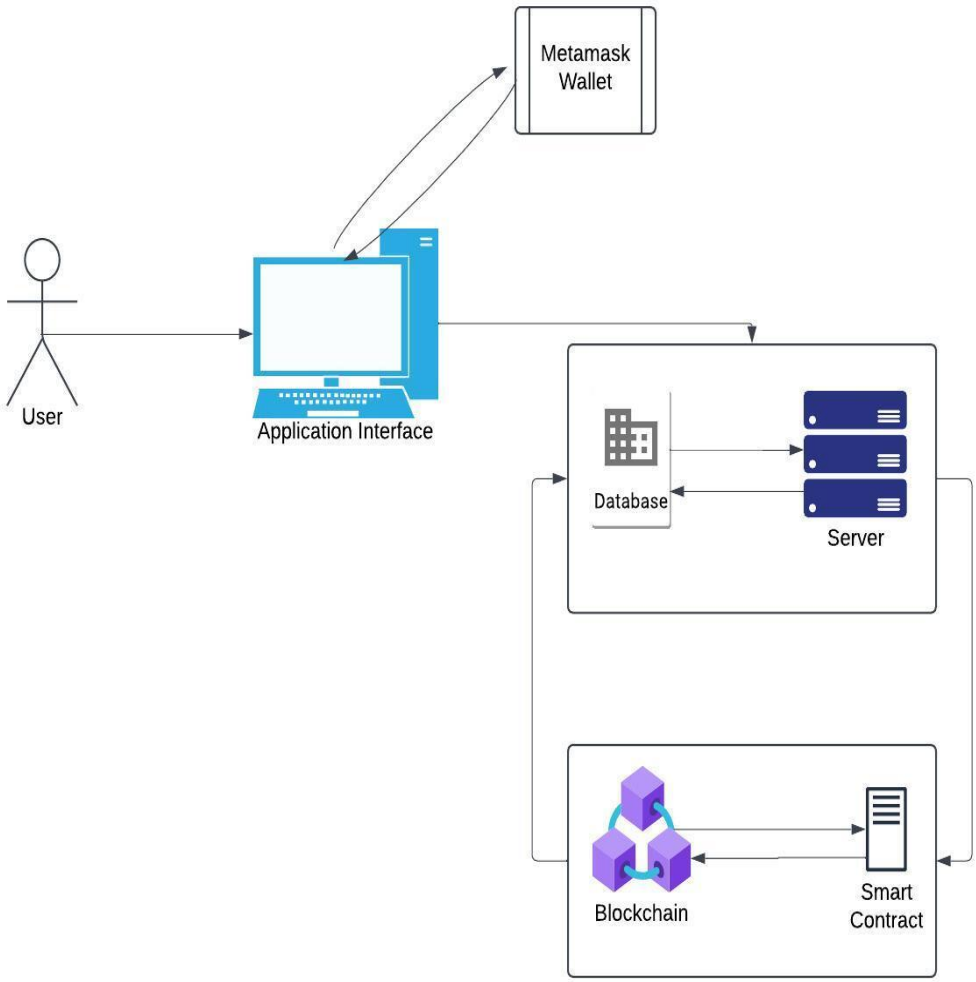

Figure 5: System Design

Voter data including Voter ID, Date of Birth, citizenship number, registered facial images, and MetaMask wallet addresses is collected during registration. Candidate information including position, party, and contest details is registered by an administrator through the admin dashboard, ensuring all entities are pre-registered and verifiable prior to election commencement.

3.2 System Workflow

The complete voting workflow is depicted in the flowchart in Figure 6. The process begins with face recognition; if unmatched, the voter is redirected for re-verification. Upon successful face match, the voter logs in using Voter ID and Date of Birth validated against the database. Successful validation triggers MetaMask wallet connection, after which the voter accesses the voting interface. The smart contract checks whether the voter has already voted;

if not, the voter selects candidates and casts the ballot, which is recorded on the blockchain. Results are fetched and displayed upon election conclusion.

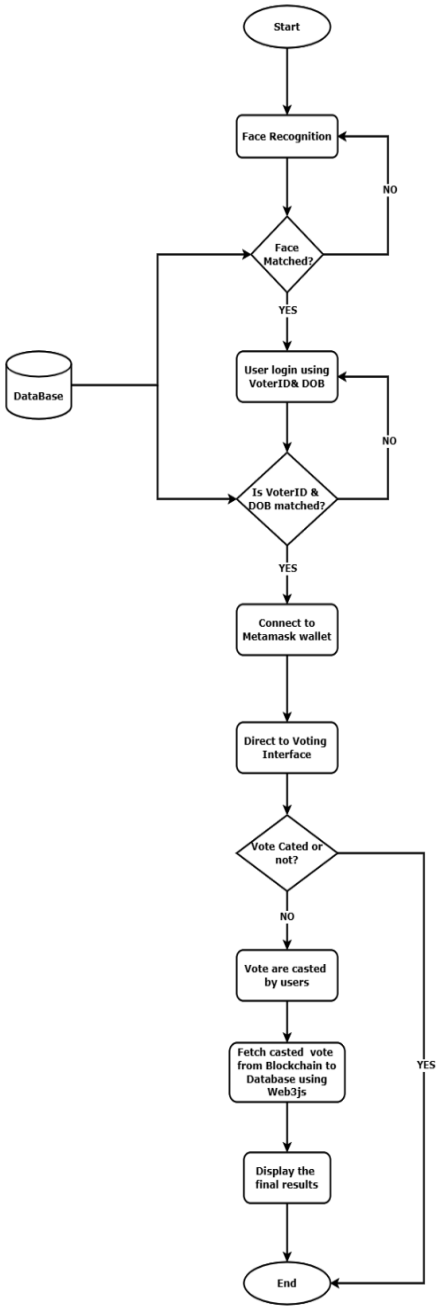

Figure 6: Flowchart

3.3 Activity Diagram and Sequence Diagram

The activity diagram in Figure 7 illustrates parallel flows in voter authentication, showing how face recognition feeds onto credential login and how the voter ID is registered on the blockchain before the voter proceeds to the voting interface. The sequence diagram in Figure 8 provides granular message exchanges between the voter,

voting system, face authentication module, database, MetaMask wallet, and blockchain across the full lifecycle from face verification to vote confirmation.

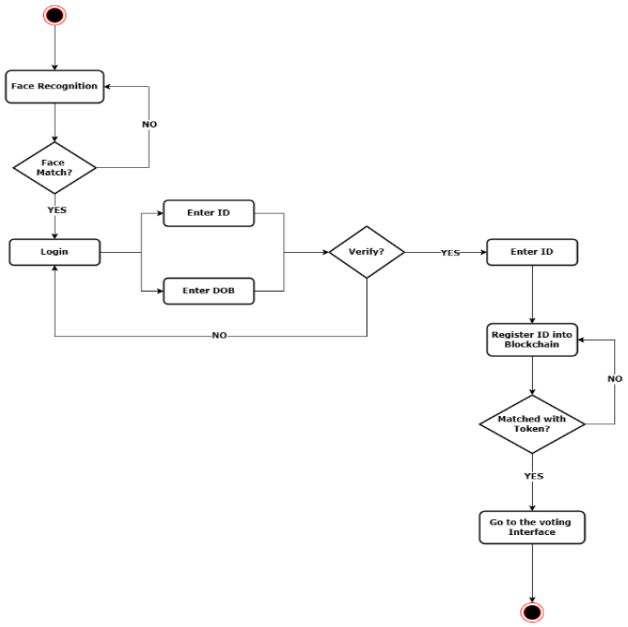

Figure 7: Activity Diagram

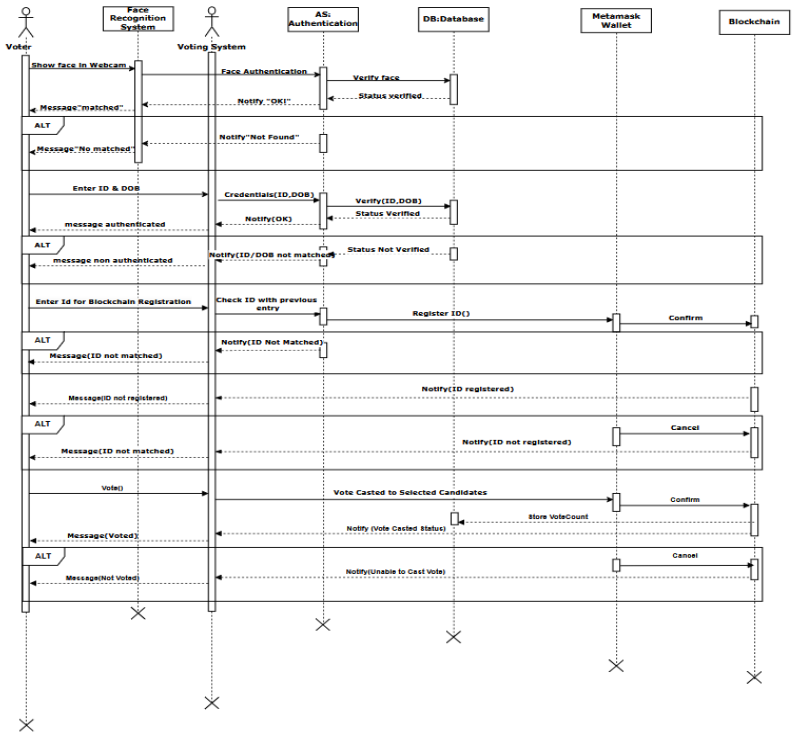

Figure 8: Sequence Diagram

3.4 Authentication Pipeline and Mathematical Justification

Voter authentication is a sequential, multi-factor pipeline. The voter's live webcam feed is processed using OpenCV, where a trained facial recognition model compares captured images against stored facial data by

computing facial feature vectors and evaluating similarity via Euclidean distance thresholding. The authentication condition is:

$$d(F(x), F(r)) = \|F(x) - F(r)\|_2 < \varepsilon \quad \text{(Equation 1)}$$

where F(x) is the feature vector of the live image, F(r) is the stored reference vector, d is the Euclidean distance, and ε is the empirically determined acceptance threshold. If satisfied, the voter proceeds to Voter ID and Date of Birth credential verification; otherwise, access is denied. MetaMask wallet connection is required before any blockchain interaction is initiated.

3.5 Smart Contract Design

Smart contracts are written in Solidity and deployed via Truffle on Ganache. The core contract maintains a mapping of voter wallet addresses to Boolean voting-status flags, and a mapping of candidate identifiers to cumulative vote counts. Upon ballot submission the contract: (1) verifies the caller's address has not previously voted; (2) validates the candidate identifier; (3) increments the candidate's vote count and marks the address as voted; and (4) emits a VoteCast event confirming the transaction. This logic is immutable once deployed, ensuring neither voters nor administrators can alter outcomes. Web3.js bridges the React-based frontend to the deployed smart contract.

Block Hash Function:

$$H(B_n) = \text{SHA-256}(B_{n-1hash} \| \text{data}_n \| \text{nonce}_n) \quad \text{(Equation 2)}$$

Tamper Detection:

$$\text{If } H(B_n) \neq H'(B_n), \text{ then block } B_n \text{ is tampered} \quad \text{(Equation 3)}$$

Chain Integrity:

$$\forall\, i \in [1, n]: \text{prevHash}_i = H(B_{i-1}) \rightarrow \text{Chain Valid} \quad \text{(Equation 4)}$$

Voting Eligibility Condition:

$$V(w_i) = \begin{cases} 1, \text{ if voted}[w_i] = \text{false} \wedge \text{eligible}[w_i] = \text{true} \\ 0, \text{ otherwise} \end{cases} \quad \text{(Equation 5)}$$

Vote Tally:

$$\text{Score}(c_j) = \Sigma_i\, V(w_i) \cdot \delta(\text{vote}(w_i), c_j) \quad \text{(Equation 6)}$$

where δ = 1 if voter i voted for candidate j, else 0

4. Results and Analysis

The system was evaluated through structured test cases covering voter authentication, ballot submission, double-vote prevention, and result display. The admin dashboard (Figure 9) provides controls for election creation, candidate registration, voter list management, and result viewing. The candidate registration interface (Figure 10) collects comprehensive candidate details. The election creation module (Figure 11) sets the smart contract address, start time, and end time for each election.

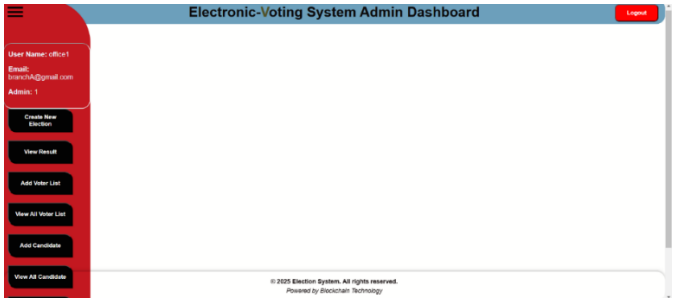

Figure 9: Admin Dashboard

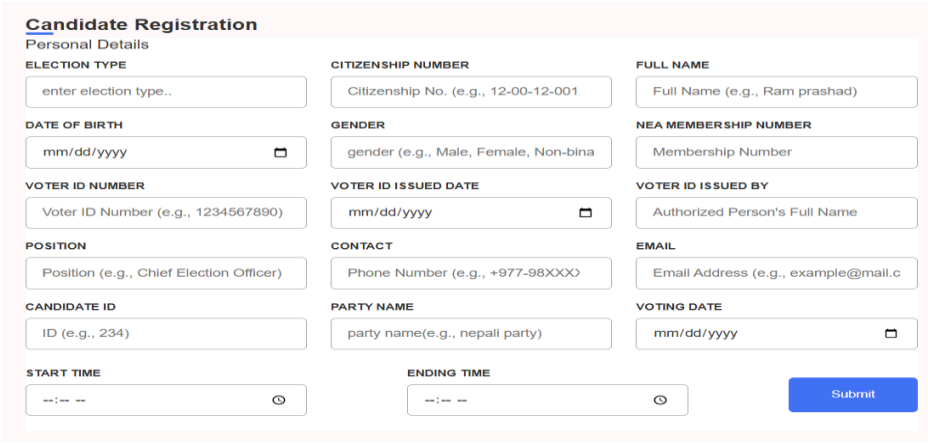

Figure 10: Candidate Registration

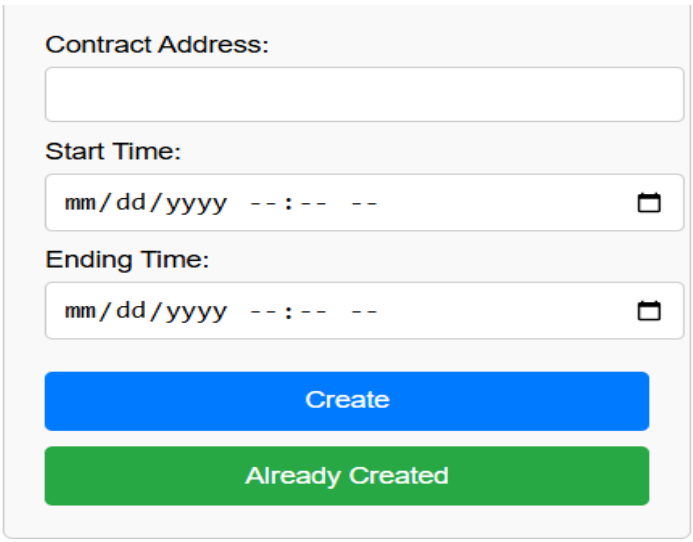

Figure 11: Create Election

Figure 12 shows the candidate list in the admin panel, confirming correct storage and retrieval of registered candidates. Election results are displayed in Figure 13, showing vote counts per candidate grouped by position (President, Treasurer), demonstrating accurate real-time tally retrieval from the smart contract via Web3.js. The user login interface is shown in Figure 14, where voters authenticate using Voter ID and Date of Birth.

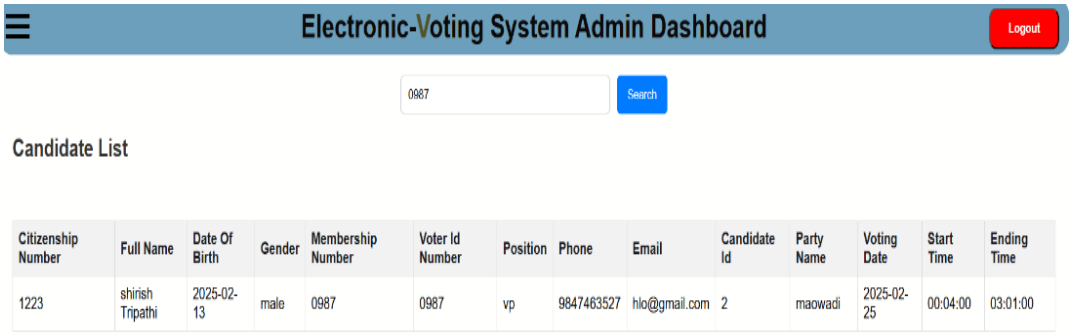

Figure 12: Candidate List

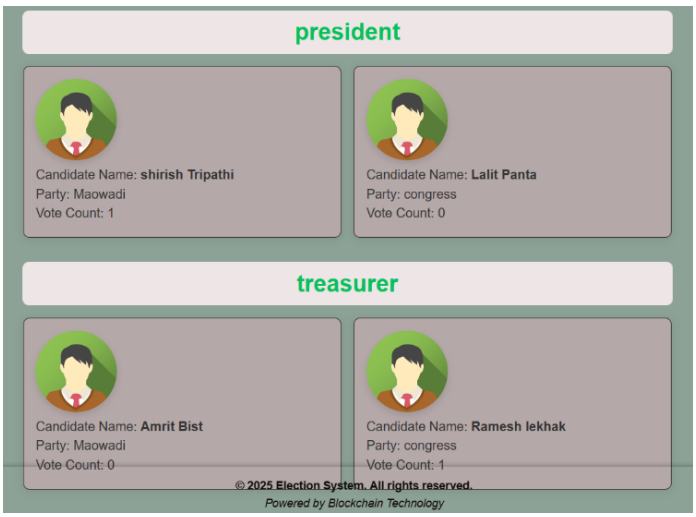

Figure 13: Result

Figure 14: User Login

Figure 15 shows the voting interface where candidates are listed by party and position. Figure 16 depicts the face recognition interface confirming the webcam-based identity verification step. Figure 17 shows the voter ID registration screen requiring voters to register their ID on the blockchain before participating.

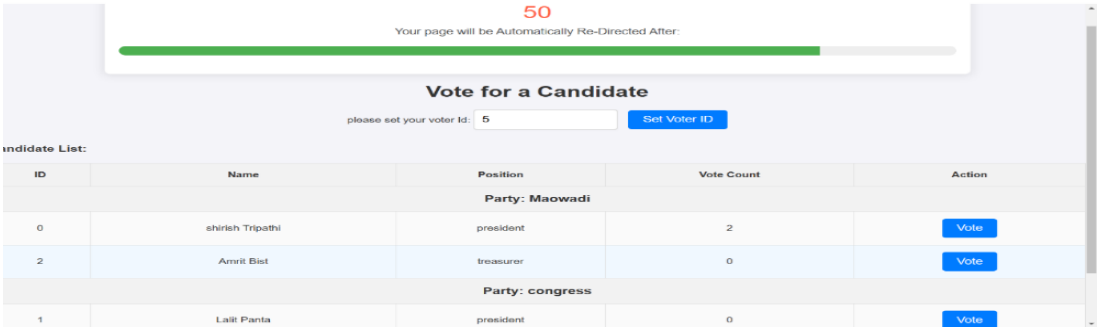

Figure 15:Vote for Candidate

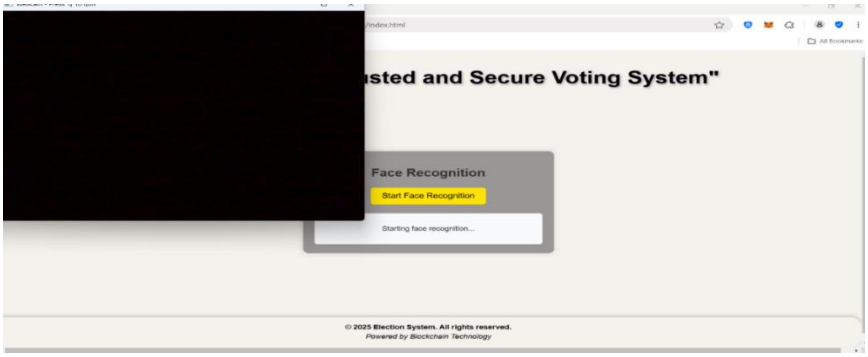

Figure 16: Face Recognition

Figure 17: Set Id

A key finding was the robustness of the multi-factor authentication pipeline: face recognition correctly denied access to unregistered faces in all test cases. The smart contract's double-voting prevention was validated by attempting a second vote from the same wallet address; the contract correctly rejected all such attempts. Vote tallies were consistent and accurate across all tests with no discrepancy between votes cast and totals reported by the smart contract. Transaction confirmation on Ganache was near-instantaneous, confirming responsive user interaction.

5. Conclusion

This work demonstrates the feasibility and effectiveness of a blockchain-based electronic voting system addressing the principal shortcomings of traditional paper-based electoral processes. The primary objective of developing a tamper-proof, transparent, and efficient e-voting platform has been fulfilled through Ethereum smart contracts, multi-factor authentication, and a responsive web interface. Smart contracts enforced the one-vote-per-user constraint without exception across all test scenarios, and the immutable blockchain ledger ensured recorded votes could not be altered by any party including system administrators. The multi-factor authentication pipeline combining facial recognition and credential verification successfully prevented unauthorized access in all evaluated cases, and transparent real-time result retrieval confirmed the system's auditability. This paper directly

responds to Nepal's growing demand for accountable and technologically transparent governance, with practical applicability to institutional elections in academic and organizational settings as well.

6. Future Enhancement

Several enhancements are identified for extending the current system. Deployment on the public Ethereum mainnet would leverage full decentralization and global accessibility, though gas fee optimization and Layer-2 scalability solutions would need to be addressed. Transformation into a fully remote voting platform accessible via mobile devices would increase participation among voters with mobility constraints or in geographically remote areas. Integrating additional biometric modalities such as fingerprint scanning or iris recognition alongside existing facial recognition would implement true multi-modal authentication, substantially reducing impersonation risk. Developing dedicated hardware voting devices running the blockchain voting software would provide a standardized, isolated environment resistant to vulnerabilities of personal computing devices. Finally, integrating zero-knowledge proof protocols would enhance voter privacy by allowing eligibility verification without exposing individual identity information on the public ledger.

References

Bagal, D., Bhosale, S., Mahajan, R. & Kale, P., 2024. E-Voting System Using Blockchain and Face Recognition. International Research Journal of Engineering and Technology (IRJET), 11(11), pp.1–10.

Berenjestanaki, M.H., Barzegar, H.R., El Ioini, N. & Pahl, C., 2024. Blockchain-Based E-Voting Systems: A Technology Review. Electronics, 13(1), p.17.

Danwar, S., Mahar, J. & Kiran, A., 2022. A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies. Computers, Materials & Continua, 72, pp.417–440.

Dowuona, R.A., 2017. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. IACR Cryptology ePrint Archive, Report 2017/110.

H.S., 2022. Blockchain 101: The Simplest Guide You Will Ever Read. [online] Available at various blockchain education platforms.

IEEE, 2025. Blockchain Integration with Multimodal Biometric Authentication for Secure E-Voting. In: Proceedings of the International Conference on Advanced Computing and Communication Systems (ICACCS). DOI: 10.1109/ICACCS61406.2025.11195074.

IOEGC-12, 2025. Blockchain-Based Electronic Voting System for Nepalese Context. In: Proceedings of the 12th IOE Graduate Conference (IOEGC-12), Paper 174. Kathmandu: Institute of Engineering.

Jafar, U., Ab Aziz, M. & Shukur, Z., 2021. Blockchain for Electronic Voting System—Review and Open Research Challenges. Sensors, 21(17), p.5874.

Pawar, A., Kale, S., Patil, S. & Jadhav, A., 2019. Blockchain-Based Electronic Voting System. In: Proceedings of the IEEE International Conference on Advanced Computing and Communication Systems (ICACCS). DOI: 10.1109/ICACCS.2019.8728467.

Rathee, G., Balasaraswathi, M., Chandran, K.P., Gupta, S.D. & Boopathi, C.S., 2021. Blockchain-Enabled E-Voting Application Within IoT-Oriented Smart Cities. IEEE Access. DOI: 10.1109/ACCESS.2020.3041824.

Singh, A. et al., 2025. Enhancing Electoral Integrity with Blockchain Technology: A Detailed Examination of E-Secure Voting Systems. IARJSET, 12(3). DOI: 10.17148/IARJSET.2025.12348.

Tas, R. & Tanriover, O.O., 2020. A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting. Symmetry, 12(8), p.1328.

Tejaswini, B.N. et al., 2025. SecureVote: A Blockchain-Based Voting System with Biometric Fingerprint Authentication. International Journal of Scientific Research in Engineering and Management (IJSREM).

Zheng, Z., Xie, S., Dai, H.N., Chen, X. & Wang, H., 2018. Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 14(4), pp.352–375.