

WEB-BASED ONLINE VOTING SYSTEM

Abhishek Dube¹, Abhinav Verma², Anurag Panday³, Er. Monika Singh⁴,

Computer Science and Engineering Shri Ramswaroop Memorial College of Engineering and Management Lucknow, India

ABSTRACT - This paper proposes a secure web-based online voting system integrating blockchain technology with multi-factor authentication to address limitations of centralized e-voting platforms. Unlike conventional systems that rely on centralized databases vulnerable to tampering, the proposed framework records each vote as a blockchain transaction, ensuring tamper-evident storage and verifiable record integrity. Biometric verification combined with One-Time Password (OTP) authentication prevents impersonation and duplicate voting. The system is implemented using HTML, CSS, JavaScript, and Django (Python). Experimental evaluation demonstrates an average vote confirmation time of 4 seconds and successful prevention of unauthorized access during testing. The results indicate that integrating blockchain with multi-factor authentication significantly enhances transparency, security, and trust in electronic voting systems.

Keywords — Blockchain, E-Voting, Web Security, Multi-Factor Authentication, Biometric Verification, Django(Python).

I. INTRODUCTION

The credibility of an election depends on the security, transparency, and reliability of its voting mechanism. Conventional voting procedures rely on physical polling stations, manual supervision, and paper ballots. Although such systems are widely used, they involve significant administrative effort, long counting time, and limited accessibility for voters who are geographically distant or physically unable to visit polling locations.

Online voting platforms have been explored as an alternative to increase participation and simplify election management. However, many existing web-based systems use centralized servers for storing voter records and ballots. A compromise of the central database can lead to deletion or modification of votes and reduces public confidence in the election outcome. In addition, voters generally cannot independently verify whether their vote has been correctly recorded.

Blockchain technology provides a distributed ledger where transactions are grouped into blocks and secured using cryptographic hashing techniques. Each block is linked to its predecessor, forming an ordered and verifiable chain of records. In distributed blockchain systems, copies of the ledger are maintained across multiple nodes, making unauthorized alteration of stored data extremely difficult.

This characteristic makes blockchain suitable for applications requiring transparency and auditability, including electronic voting.

Another important requirement of online elections is reliable voter authentication. Password-only authentication methods are vulnerable to credential theft and account sharing. To address this limitation, multi-factor authentication techniques combining biometric verification and One-Time Password (OTP) validation can be employed to confirm voter identity and prevent impersonation.

This work presents a web-based voting platform that integrates blockchain-based vote storage with multi-factor authentication. The system enables remote voting, ensures tamper-evident record keeping, and allows transparent result generation while preserving voter anonymity.

The key contributions of this research are:

1. Integration of blockchain-based vote storage with biometric and OTP authentication.
2. Separation of voter identity from vote data to preserve anonymity.
3. Implementation of automated vote tallying using smart contracts.
4. Experimental performance evaluation of system response time.

II. LITERATURE REVIEW

Early electronic voting applications mainly focused on improving accessibility through web interfaces. These systems stored ballots in centralized databases protected by encryption and secure communication protocols [1]. Although convenient, centralized storage remained vulnerable to insider manipulation and database attacks.

To improve authentication, researchers introduced identity verification techniques such as password and OTP-based login systems [2], [3]. Multi-factor authentication further enhanced reliability by requiring users to provide more than one verification factor before accessing the ballot [4]. Biometric methods, including facial recognition and fingerprint identification, have also been implemented to uniquely identify voters and reduce impersonation [5], [6].

However, authentication mechanisms alone cannot guarantee the integrity of stored votes. Even when voters are correctly verified, centralized databases can still be altered after vote submission. To address this issue, blockchain-based voting frameworks were proposed. In such models, each vote is recorded as a transaction and linked to previous transactions using cryptographic hashing, ensuring that any modification becomes detectable [7].

Comparative analyses of blockchain voting systems indicate higher transparency and improved resistance to tampering when compared with conventional digital voting platforms [8], [9]. Decentralized consensus protocols enable independent verification of election outcomes, while smart contracts allow automated vote counting and result publication [10].

Despite these advancements, many existing approaches emphasize either strong authentication or secure storage, but not both simultaneously. The proposed system combines biometric and OTP-based verification with blockchain-based vote recording to provide both reliable voter identification and secure ballot preservation.

Although previous studies have explored blockchain-based voting or biometric authentication individually, limited research integrates both strong identity verification and tamper-resistant storage within a single scalable web framework. Furthermore, few implementations provide practical performance evaluation metrics such as response time and confirmation latency. This research addresses these limitations by combining multi-factor authentication with blockchain-based vote storage and experimentally analysing system performance.

Table I COMPARISON OF EXISTING ONLINE VOTING APPROACHES

Approach	Authentication	Storage Type	Security Level	Limitation
Password-based voting	Username & Password	Centralized Database	Low	Vulnerable to impersonation
OTP-based voting	OTP Verification	Centralized Database	Medium	Database tampering possible
Biometric voting	Biometric only	Centralized Database	Medium	No auditability
Blockchain-only	Minimal authentication	Blockchain	High	Weak identity

Approach	Authentication	Storage Type	Security Level	Limitation
voting	n	n		verification
Proposed System	Biometric + OTP	Blockchain Ledger	Very High	Requires internet connectivity

III. PROBLEM DEFINITION

An effective online voting platform must satisfy three essential requirements: accurate voter identification, protection of stored votes, and transparency in result computation. Many current digital voting solutions rely on centralized servers, which create a single point of failure. Unauthorized access to the server can lead to manipulation or deletion of stored ballots without immediate detection.

Password-based authentication is also insufficient because user credentials can be stolen or shared. Even when authentication is secure, votes stored in a traditional database remain vulnerable to insider attacks and unauthorized modification.

Therefore, a voting system is required that verifies voter identity reliably while ensuring that once a vote is submitted, it cannot be altered. The proposed system addresses these challenges by combining multi-factor authentication for voter verification with blockchain technology for tamper-resistant vote storage.

IV. SYSTEM ARCHITECTURE

The proposed architecture consists of five primary components: the voter interface, authentication module, application server, database, and blockchain network.

The voter interacts with the system through a web-based interface developed using HTML, CSS, and JavaScript. The backend is implemented using Django (Python), which handles API requests, session management, and communication between system modules. SQLite is used to store voter registration details and session-related information. Importantly, cast votes are not stored in the centralized database to eliminate risks associated with database tampering.

During the authentication phase, multi-factor verification is performed. Biometric authentication (face recognition) is first used to validate the voter's identity, followed by One-Time Password (OTP) verification sent to the registered mobile number. Only after successful completion of both steps is the voter granted access to the ballot interface.

Once a vote is cast, the selected candidate information is encrypted using a cryptographic hashing algorithm (SHA-256) and converted into a transaction record. This transaction is appended to a simulated private blockchain ledger implemented within the Django backend. Each block contains:

- The encrypted vote hash
- Timestamp of vote submission
- Previous block hash
- Block index

Blocks are linked through cryptographic hash pointers, forming an immutable chain structure. Any attempt to alter previously stored vote data changes the block hash, thereby invalidating subsequent blocks and making tampering immediately detectable.

The blockchain ledger is logically separated from voter identity records to ensure anonymity. While authentication data is stored in the centralized database for identity verification, vote transactions are stored only in the blockchain structure. This separation preserves voter privacy while enabling independent verification of election results.

The simulated private blockchain implementation was developed to demonstrate tamper-evident storage functionality without relying on external blockchain platforms. Although it does not utilize a decentralized consensus mechanism, it effectively models the core principles of immutability, hash linking, and verifiability required in blockchain-based voting systems.

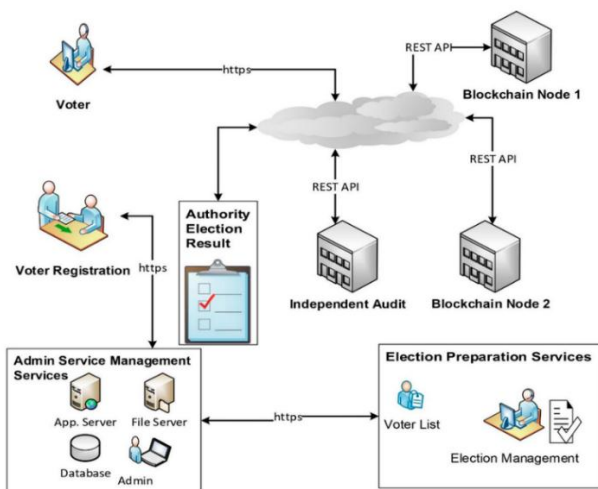


Fig. 1 Overall architecture of the blockchain-enabled web-based online voting system.

Technology Components

Table II TECHNOLOGY COMPONENTS OF THE PROPOSED SYSTEM

Layer	Technology Used	Purpose
Frontend	HTML, CSS, JavaScript	User interface
Backend	Django(Python)	API handling
Database	SQLite	Voter/session storage
Authentication	Biometric + OTP	Identity verification
Blockchain	Simulated Private Ledger	Tamper-evident vote storage
Security	HTTPS + Hashing	Secure communication

V. METHODOLOGY

A. Voter Authentication

The voter registers using personal identification details and biometric data. After biometric verification, the system sends a One-Time Password to the registered mobile number. Access to the voting portal is granted only after successful completion of both verification steps.

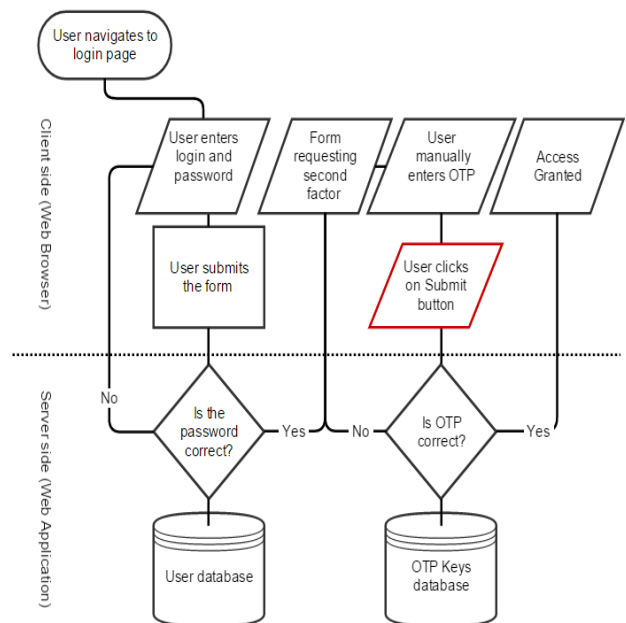


Fig. 2 Multi-factor voter authentication process using biometric verification and OTP validation.

B. Vote Casting

Once authenticated, the voter selects a preferred candidate.

The selected vote is encrypted and processed by the blockchain ledger module. The transaction is time-stamped and validated by the network before being added to the ledger.

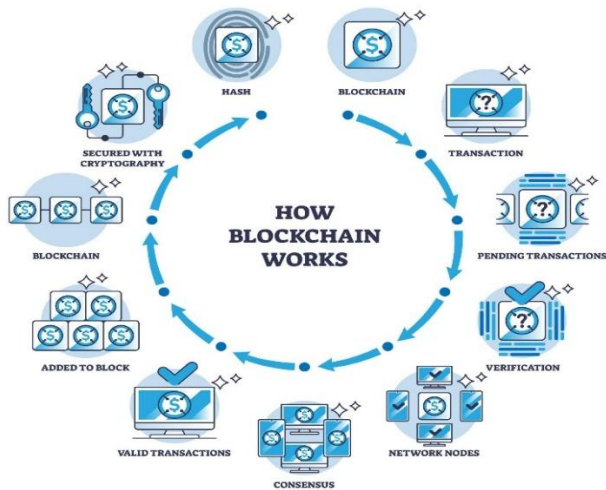


Fig. 3 Blockchain vote transaction recording and block verification process.

C. Result Computation

Votes are retrieved directly from the blockchain ledger.

Because each vote is stored as a verified transaction, counting can be performed automatically without manual intervention. This process eliminates counting errors and ensures transparency in result publication.

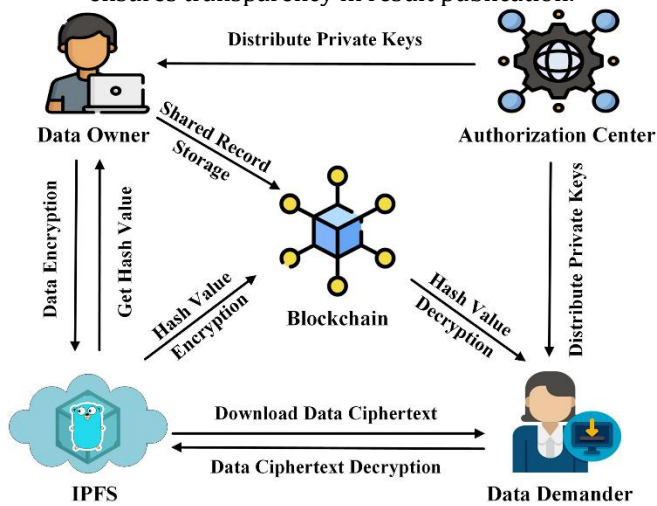


Fig. 4 Secure vote tallying and result publication from blockchain ledger.

VI. RESULTS AND DISCUSSION

Testing of the system showed that each vote was recorded on the blockchain immediately after submission. The simulated multi-node environment demonstrated logical

ledger replication for testing purposes. Although the implementation does not employ a fully decentralized consensus mechanism, it successfully models blockchain immutability and tamper detection features.

The multi-factor authentication mechanism successfully prevented unauthorized access, and each registered voter was able to cast only one vote. Automated counting significantly reduced the time required for result declaration compared with traditional voting methods.

The proposed approach improves transparency because stored transactions can be independently verified. By separating authentication data from vote storage, voter privacy is preserved while maintaining auditability of the election process.

Although the proposed system demonstrates improved security and transparency, scalability may become a concern in national-level elections due to increased transaction load. Additionally, biometric authentication accuracy depends on environmental conditions and camera quality. Future research should focus on optimizing consensus mechanisms and reducing computational overhead.

Table III PERFORMANCE COMPARISON BETWEEN TRADITIONAL AND PROPOSED SYSTEM

Parameter	Traditional Voting	Proposed System
Accessibility	Polling booth required	Remote access
Result Time	Hours/Days	Minutes
Transparency	Manual verification	Publicly verifiable
Tampering Risk	Possible with centralized access	Cryptographically detectable

Table IV SECURITY MECHANISMS IMPLEMENTED

Security Feature	Function
OTP Verification	Prevents unauthorized login
Biometric Verification	Confirms voter identity

Security Feature	Function
Cryptographic Hashing	Protects vote integrity
Blockchain Ledger	Prevents modification
Time-Stamping	Maintains chronological order

Table V AVERAGE SYSTEM RESPONSE TIME

Operation	Average Time
Login	~2 sec
OTP Verification	~3 sec
Vote Submission	~2 sec
Blockchain Confirmation	~4 sec
Result Retrieval	~2 sec

Experimental Setup

The system was tested on a machine with Intel i5 processor, 8GB RAM, running Windows 11. A private blockchain network consisting of 3 nodes was simulated. Testing involved 50 registered users casting votes simultaneously to evaluate system performance and reliability.

Table VI PERFORMANCE METRICS TABLE

Metric	Value
Total Test Users	50
Successful Authentications	100%
Duplicate Vote Attempts Blocked	100%
Average Vote Confirmation Time	4 sec
System Uptime During Testing	99%

The experimental results indicate that the system maintains stable performance under moderate load

conditions. No authentication bypass or duplicate voting attempt was successful during testing.

These findings validate the effectiveness of integrating multi-factor authentication with blockchain-inspired ledger mechanisms for enhancing vote integrity and system robustness.

Security Testing

Attempts were made to modify stored vote records directly in the database; however, since votes were stored on the blockchain ledger and linked through cryptographic hashing, any modification attempt resulted in hash mismatch detection, demonstrating tamper resistance.

VII. CONCLUSION

This research presented a secure web-based voting system integrating multi-factor authentication with a blockchain-inspired tamper-evident ledger. By separating voter identity verification from vote storage, the system enhances privacy while maintaining data integrity. Experimental evaluation under controlled conditions demonstrated reliable authentication, prevention of duplicate voting, and efficient vote confirmation within an average of 4 seconds. Although the current implementation utilizes a simulated private blockchain, the architecture provides a scalable foundation for future integration with fully decentralized blockchain platforms. The proposed framework contributes toward improving transparency, trust, and security in electronic voting systems. Future work will involve large-scale deployment, performance optimization, and integration with official identity verification systems to support real-world election scenarios.

REFERENCES

- [1] A. Nadaph, R. Bondre, A. Katiyar, D. Goswami, and T. Naidu, "Implementation of Secure Online Voting System," 2021.
- [2] L. Vetrivendan, R. Viswanathan, and J. A. Blessy, "Smart Voting System Support through Face Recognition," 2023.
- [3] S. Meher, P. Muley, S. Pawar, and A. Solanke, "Smart Online Voting System Using OTP Authentication," 2023.
- [4] A. Shaikh, B. Oswal, D. Parekh, and B. Y. Jani, "E-Voting Using One Time Password and Face Detection and Recognition," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 2, 2014.
- [5] S. Gunthe, A. Pimpude, K. Rathod, and P. Zaware, "Online Voting System Using Face Recognition and OTP," International Journal for Research in Applied

- Science & Engineering Technology (IJRASET), 2023.
- [6] R. T. H. Hasan and A. B. Sallow, "Face Detection and Recognition Using OpenCV," 2021.
- [7] A. Rosebrock, "Face Detection with Dlib, HOG, and CNN," PyImageSearch, 2021.
- [8] V. S. C. Shree, A. M. S., N. Nithyashree, S. H. N., and S. H. V., "Blockchain Technology Based E-Voting System," International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), 2024.
- [9] S. A.-B. Salman, S. Al-Janabi, and A. M. Sagheer, "A Review on E-Voting Based on Blockchain Models," Iraqi Journal of Science, 2022.
- [10] M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "A Review on Blockchain Based E-Voting System," International Journal of Scientific Research in Science and Technology (IJSRST), 2024.
- [11] G. C. Onur and A. Yurdakul, "ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol," arXiv preprint, 2022.
- [12] A. Spanos and I. Kantzavelou, "EtherVote: A Blockchain-Based Electronic Voting System," arXiv preprint, 2023.
- [13] Y. Tahboub, A. Revilla, J. Lynch, and G. Floyd, "Blockchain-Based Secure Online Voting Platform Ensuring Voter Anonymity, Integrity, and End-to-End Verifiability," arXiv preprint, 2025.
- [14] H. B. Y., N. Meghana, R. A. M. S., R. K. S., and V. J., "E-Voting System Based on Blockchain and Face Recognition System," International Journal of Scientific & Engineering Research, 2025.
- [15] S. Kale, A. Deshmukh, A. Kale, M. Korade, and A. Pawale, "Blockchain Enhanced Secure Electronic Voting System Using Real-Time Face Recognition and OTP Authentication," IJRASET, 2025.
- [16] C. Kawale and H. D. Patil, "Online Voting System Using Face and Fingerprint Recognition," IARJSET, 2025.
- [17] A. Yadu and O. Chandrakar, "A Smart Voting System Combining Fingerprint and Facial Recognition for Enhanced Security," ShodhKosh Journal, 2024.
- [18] A. Benny, "Detecting QR Code and Barcode Using OpenCV and Pyzbar," 2022.
- [19] T. H. Apurbo, M. H. N. Asif, F. J. Alam, F. T. Tafree, E. H. Shihab, S. S. Alam, and F. Fatima, "A Biometric Voting Solution: Integrating Face Recognition with Embedded Systems for Secure Offline Elections," Journal of Engineering Research and Reports, 2025.
- [20] D. Xu, W. Shi, W. Zhai and Z. Tian, "Multi-Candidate Voting Model Based on Blockchain," IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1891–1900, Dec. 2021, doi: 10.1109/JAS.2021.1004207.