© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723487

Decentralized Privacy-Preserving E-Voting System Using Blockchain and Zero-Knowledge Cryptography

SARIYA ANJUM[1], DHARINI N[2], DHRUTHI HR[3], DHUSHYANTH DAYANAND[4], MANU MN[5]
[1]*Asst Professor, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India.*
[2,3,4,5]*Student, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India.*

Abstract*— Electronic voting can provide convenient participation and faster election management, but a secure digital voting system must address voter authentication, duplicate voting, privacy, vote integrity, and trust in election records. This paper presents a decentralized privacy-preserving e-voting system using blockchain and zero-knowledge cryptography with facial recognition for voter verification. The proposed system combines voter registration and login, facial verification, candidate and election management, secure vote casting, duplicate-vote prevention, blockchain-oriented transaction recording, vote counting, and result generation. Facial recognition and liveness verification provide an additional identity-verification layer before a voter accesses the ballot. Blockchain is used to provide a tamper-evident record of voting transactions, while zero-knowledge cryptographic techniques are intended to support verification without unnecessarily revealing sensitive voter information. A web-based prototype demonstrates the integration of these security and privacy mechanisms into a unified voting workflow.

Keywords*— E-Voting, Blockchain, Zero-Knowledge Cryptography, Facial Recognition, Voter Verification, Privacy, Duplicate Voting, Secure Voting, Election Management

I. INTRODUCTION

Electronic voting has evolved as an alternative to conventional election processes because digital platforms can reduce manual effort, improve accessibility, and support faster vote counting. At the same time, moving an election process online introduces important security and privacy requirements. A voting platform must ensure that only eligible users can access the ballot, that a voter cannot cast multiple votes, that voting records are protected from unauthorized modification, and that sensitive voter information is not unnecessarily exposed.

Blockchain technology provides a distributed ledger in which transactions are linked and can be made tamper-evident. Zero-knowledge cryptography provides a method for proving that a statement is true without revealing the underlying secret information. Facial recognition adds another layer of identity verification and can help reduce impersonation attempts. The combination of these technologies provides a multi-layer approach to secure and privacy-preserving electronic voting.

The proposed system integrates voter registration, login, facial verification, candidate selection, vote casting, duplicate-vote prevention, secure transaction recording, and election result generation in one web-based platform.

The design is motivated by the need to separate three concerns that are often treated as one: identity assurance, ballot privacy, and transaction integrity. Facial verification addresses identity assurance; zero-knowledge cryptography addresses privacy-preserving proof; and blockchain addresses the integrity and auditability of recorded transactions.

Objectives

- To develop a secure online voting platform.
- To verify voter identity using facial recognition and liveness checking.
- To prevent unauthorized and duplicate voting.
- To provide privacy-preserving verification using zero-knowledge cryptographic techniques.
- To record voting transactions using blockchain-oriented mechanisms.
- To provide administrator functions for candidate and election management.
- To automate vote counting and result generation.
-

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723487

II. METHODOLOGY

The proposed system follows a sequential web-based voting workflow. The voter first registers an account and enrolls facial information. During voting, the voter logs in and provides the required voter identifier. The facial verification module activates the camera and performs face detection, single-person checking, liveness detection, and face matching. If verification succeeds, the voter is permitted to proceed to the election interface.

After successful verification, the voter is shown the available election and candidates. The voter selects a candidate and submits the ballot. Before accepting the vote, the system checks the voter's voting status to prevent repeated voting. The accepted vote is processed by the backend and passed to the transaction-recording layer.

The blockchain component is intended to provide a tamper-evident record of the voting transaction. The privacy layer uses zero-knowledge cryptographic concepts so that required properties can be verified without unnecessary disclosure of private information. The final stage counts the accepted votes and makes the candidate-wise result available to the administrator.

The complete workflow therefore consists of registration, authentication, facial verification, election display, candidate selection, vote casting, transaction recording, duplicate-vote prevention, and result generation.

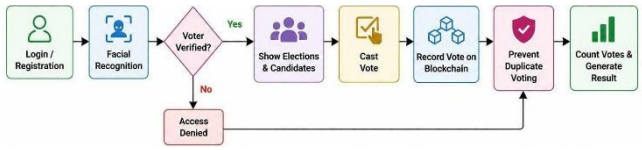

Figure 1: Flowchart of the proposed e-voting system.

The flowchart emphasizes that facial verification is a gate before the ballot becomes available. If verification fails, access is denied; if verification succeeds, the voter proceeds through candidate selection and voting. The subsequent transaction and voting-status checks are part of the secure voting workflow.

III. MODELING AND ANALYSIS

The proposed e-voting system is organized into functional layers consisting of the user layer, client application, backend services, data layer, blockchain layer, and privacy layer. The voter interacts with the client application for registration, login, face capture, verification, candidate selection, and vote confirmation. Backend services perform authentication, voter verification, voting validation, and transaction processing.

The facial verification workflow contains four principal checks. Face detection confirms the presence of a face. The single-person check verifies that the expected number of people are present. Liveness detection is intended to distinguish a live user from a simple presentation attack such as a static image. Face matching compares the captured face with the registered identity.

The prototype interface presents these checks explicitly to the user. This makes the verification stage understandable and gives a visible indication that identity and liveness checks form part of the voting process.

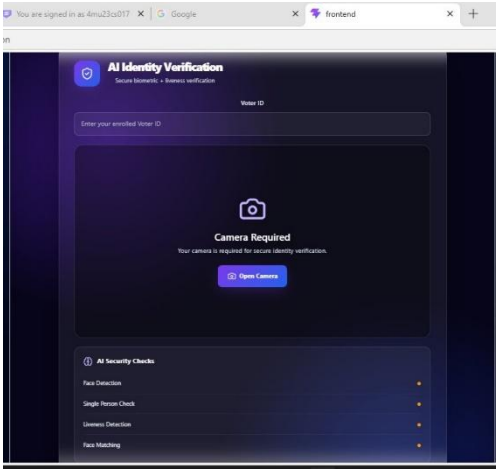

Figure 2: AI identity verification interface showing camera access and security checks.

The displayed verification interface includes fields for the enrolled voter ID, camera activation, and security checks for face detection, single-person checking, liveness detection, and face matching. This interface is used as the identity-verification stage before voting.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723487

Table 1: System Modules and Their Functions

Module	Function
Voter Registration	Creates voter account and enrolls identity information.
Facial Verification	Performs face detection, liveness and identity matching.
Election / Candidate	Displays candidates and supports candidate management.
Voting	Allows a verified voter to select and cast one ballot.
Blockchain	Records voting transaction information in a tamper-evident manner.
Duplicate Prevention	Checks voting status to prevent repeated voting.
Results	Counts votes and generates candidate-wise results.

The application layer communicates with backend services through defined API operations. Authentication services handle login and account validation. The voter verification service receives the required voter information and performs the identity-verification workflow. The voting service validates the ballot request and checks whether the voter is permitted to cast a vote. The transaction service prepares the voting transaction for the blockchain-oriented layer.

The database maintains application information required by the system, including voter information, candidate information, election details, voting status, and operational records. The blockchain layer is separated conceptually from the application database so that the application data and the transaction record can serve different purposes.

A privacy-preserving voting design should avoid unnecessarily exposing the relationship between a voter's real-world identity and the selected candidate. Zero-knowledge techniques are therefore considered at the verification layer. A proof can establish that a required condition is satisfied without directly revealing the secret value used to satisfy that condition.

The system also separates administrator operations from voter operations. The administrator interface is used for candidate management and result viewing, while the voter interface is restricted to the functions needed for registration, verification, and voting.

IV. PROPOSED SYSTEM

The proposed system is designed to overcome important limitations of conventional electronic voting by integrating identity verification, privacy-preserving cryptography, and blockchain-based recording. A registered voter first logs into the web application and then completes facial verification using the camera. If the voter is successfully verified, the election interface becomes available.

The voting interface displays candidate information and allows the voter to select one candidate. The voter then proceeds to the secure ballot workflow. The backend validates the request and checks voting status. If the voter has not previously voted, the system accepts the ballot and passes the transaction to the recording layer.

The administrator has a separate authenticated interface. The administrator can manage candidates and view election results. This separation reduces the exposure of administrative functions to normal voters and provides a clear distinction between election management and ballot casting.

IV. PROPOSED SYSTEM (Continued)

The proposed architecture contains an application layer and a set of backend services. The application layer provides face capture, face recognition, voting interface, and vote confirmation. Backend services handle authentication, voter verification, voting, and transaction processing. The blockchain network represents the decentralized transaction-recording component, while the database supports application-level records.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723487

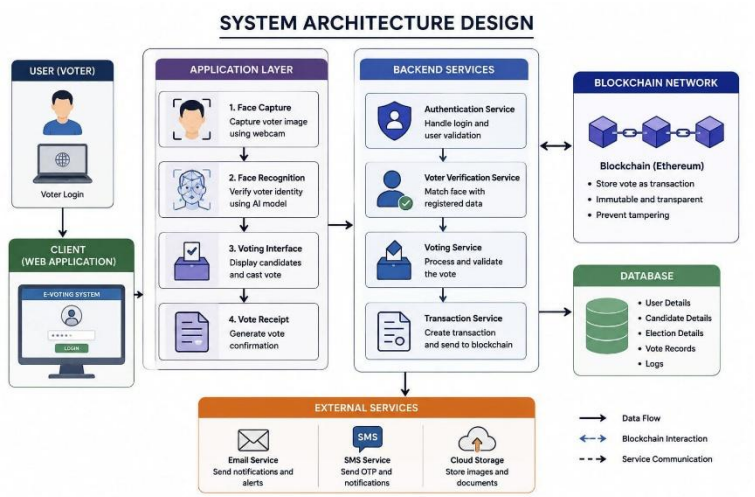

Figure 3: System architecture showing the client application, backend services, blockchain network and database.

The architecture also illustrates the separation between the voter, client web application, backend services, blockchain network, and database. Data flows from the voter through the application and backend services, while blockchain interaction is treated as a separate transaction path. This layered arrangement supports modular implementation and makes individual components easier to test and improve.

The facial-recognition stage is connected to the voter-verification service rather than directly to the ballot. This means that a successful identity-verification result is used as a prerequisite for voting. The design therefore places biometric verification before candidate selection and vote submission.

V. EXISTING SYSTEM

Traditional voting systems generally require voters to attend designated polling locations and depend on physical identification, election personnel, ballot handling, and manual or centralized counting procedures. These processes can involve significant operational effort and may make remote participation difficult.

Conventional online voting systems may depend heavily on centralized application servers and databases. When authentication, vote storage, and counting are controlled by one trusted system, voters must depend on that authority for the integrity of the complete process. Systems using only passwords may also face risks related to credential sharing, theft, or impersonation.

Some electronic voting designs use centralized databases to maintain voter status and vote records. Although such designs can be efficient, the integrity of the complete election depends strongly on the security and administrative control of the central system.

The proposed system addresses these limitations by combining facial verification with liveness checking, duplicate-vote status checking, blockchain-oriented transaction recording, and a zero-knowledge privacy layer. The objective is to distribute security responsibilities across multiple mechanisms rather than relying on a single authentication or storage method.

Table 2: Comparison Between Existing and Proposed System

Feature	Existing System	Proposed System
Voting Access	Physical / centralized online	Web-based secure workflow
Identity Verification	Manual / password based	Facial verification + liveness
Duplicate Voting	Manual / centralized check	Application voting-status check
Privacy	Depends on system design	Zero-knowledge privacy layer
Vote Record	Centralized / conventional	Blockchain-oriented record

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1723487

Result Generation	Manual or centralized	Automated candidate-wise results

VI. IMPLEMENTATION

The frontend of the prototype is developed using React with CSS-based styling and React Router for navigation. The backend uses Python and FastAPI to provide application programming interfaces for authentication, voter operations, candidate operations, voting operations, and result retrieval. A database layer stores the application data required by these services.

The AI identity component uses the facial-analysis stack included in the project technology set. The camera-based interface captures the voter image, while the verification service performs the defined checks. The blockchain and zero-knowledge components form the security-oriented architecture for transaction integrity and privacy-preserving verification.

The administrator module provides an authenticated entry point. Candidate management functions allow the administrator to add or remove candidates and maintain the election candidate list. The results module retrieves vote information and displays candidate-wise counts and percentages.

VI. IMPLEMENTATION (Continued)

The voter registration module collects the required voter information and provides a face-enrollment step. The login module authenticates the registered voter before the verification workflow. Once the face verification process is completed successfully, the voter dashboard displays the current identity and voting status.

The voter dashboard presents the election and candidate information in a card-based interface. Candidate selection is performed before the secure ballot step. The application maintains a voting-status state so that the same voter is not permitted to complete another ballot through the normal workflow after a successful vote.

The administrator login is separated from the voter login. Administrative access is protected by an administrator authentication screen. The administrator dashboard provides election-management functions, while the results page presents candidate-wise vote counts and related election information.

VII. SECURITY AND PRIVACY

Security in the proposed system is achieved through multiple layers. Account authentication restricts access to registered users. Facial recognition adds a biometric identity layer. Liveness detection is intended to reduce simple presentation attacks. The single-person check helps ensure that the verification scene contains the expected user before the identity comparison is completed.

Duplicate-vote prevention is handled through the voting-status check. Before a vote is accepted, the system verifies that the voter has not already completed the voting operation. This mechanism is complementary to identity verification because confirming who the voter is and confirming whether that voter has already voted are separate security conditions.

Blockchain addresses transaction integrity rather than identity. A blockchain ledger can make recorded transactions tamper-evident and can provide an auditable sequence of transactions. Zero-knowledge cryptography addresses privacy by allowing a verifier to check a statement without receiving the secret information itself.

In a production election system, biometric information, cryptographic keys, smart contracts, network nodes, and administrative privileges would require additional protection and independent security assessment. The current work therefore presents these components as an academic prototype and architectural demonstration.

VIII. RESULTS AND DISCUSSION

The proposed system was implemented as a web-based prototype and exercised through the major voter and administrator interfaces. The registration interface provides account creation and facial enrollment. The AI identity-verification interface provides camera access and displays checks for face detection, single-person detection, liveness detection, and face matching.

The voter dashboard provides identity status, voting

status, privacy status, and candidate selection. The candidate interface allows the voter to select a candidate before proceeding to the secure ballot. These screens demonstrate the user-facing workflow of the proposed system.

The administrator interface provides a separate login and protected access to election-management functions. Candidate management and result viewing are handled through the administrator workflow. This demonstrates the separation between voter-facing and administrative operations.

The prototype demonstrates the intended sequence from registration and identity verification through candidate selection, vote processing, duplicate-vote prevention, and result generation. The system is therefore suitable for demonstrating the integration of the main modules in an academic project environment.

The current evaluation is functional rather than a controlled scientific benchmark. Therefore, numerical facial-recognition accuracy, frame rate, latency, or security percentages are not reported as experimental results. Such measurements should only be included after systematic testing with a defined dataset, hardware configuration, sample size, and evaluation procedure.

Advantages

- Multi-layer voter verification through account authentication and facial verification.
- Privacy-oriented design using zero-knowledge cryptographic concepts.
- Tamper-evident transaction recording through blockchain architecture.
- Duplicate-vote prevention through voting-status checking.
- Separate voter and administrator interfaces.
- Automated candidate-wise result generation.

Limitations

The present work is an academic prototype and should not be interpreted as a production-ready public-election system. A production deployment would require formal security analysis, independent audits, secure key management, privacy assessment, legal and electoral compliance, strong anti-spoofing evaluation, scalability testing, and end-to-end verification.

IX. FUTURE ENHANCEMENT

Future development can extend the prototype with complete deployment and testing of the blockchain and zero-knowledge components. Smart contracts can be formally tested and audited before deployment. Zero-knowledge circuits can be formally verified so that the privacy guarantees of the voting protocol can be evaluated independently.

The facial-verification component can be evaluated with a larger and more diverse test set under different lighting, camera, pose, and presentation-attack conditions. Additional anti-spoofing methods can be studied to strengthen liveness verification. Performance benchmarking can measure verification time, transaction time, throughput, and scalability.

Future versions can also investigate decentralized identity management, secure cryptographic-key storage, end-to-end verifiability, accessibility improvements, audit interfaces, and controlled multi-node blockchain deployment. These enhancements would move the system from a prototype toward a more comprehensive research platform.

X. CONCLUSION

The proposed decentralized privacy-preserving e-voting system integrates blockchain, zero-knowledge cryptography, and facial recognition to address important security and privacy requirements in electronic voting. The system combines voter registration, authentication, facial verification, candidate selection, duplicate-vote prevention, secure transaction recording, administrator management, and automated results into a unified workflow.

Facial verification provides an additional identity layer before ballot access. Blockchain provides a tamper-evident transaction model for recorded voting activity, while zero-knowledge cryptography provides a foundation for privacy-preserving verification. The separation of voter and administrator functions further organizes the election workflow.

The prototype demonstrates the feasibility of integrating these technologies in a web application.

Further development and controlled evaluation are required before any real-world election deployment, particularly in the areas of formal cryptographic verification, security auditing, scalability, privacy protection, and legal compliance.

XI. LITERATURE SURVEY

Research on blockchain-based voting has explored the use of distributed ledgers and cryptographic proofs to improve transparency, integrity, and public verifiability. Yang et al. proposed a publicly verifiable online voting protocol without a trusted tallying authority and studied properties including eligibility, uniqueness, privacy, integrity, correctness, and end-to-end verifiability [1].

Li et al. studied a blockchain-based self-tallying voting protocol in decentralized IoT. Their work considers decentralization and voting properties such as ballot secrecy, fairness, and dispute-freeness [2]. These studies motivate the use of blockchain and cryptographic protocols as components of secure electronic voting.

Other published work has investigated combining blockchain with facial recognition. Such approaches use biometric verification to strengthen voter authentication while blockchain provides transaction storage [3], [4]. Recent research has also explored facial-recognition and blockchain combinations for improving electoral integrity and accessibility [5].

The proposed project differs in its emphasis on privacy-preserving verification through zero-knowledge cryptography in addition to facial verification and blockchain-oriented recording. The literature survey therefore supports the selection of complementary mechanisms rather than relying on one security technology.

XII. PRIVACY-PRESERVING VERIFICATION

Zero-knowledge cryptography allows a prover to demonstrate knowledge of a secret or satisfaction of a condition to a verifier without revealing the secret itself. In an e-voting context, this concept can be applied to statements such as eligibility or validity, depending on the precise circuit and protocol design.

The separation between identity verification and ballot privacy is important. Facial recognition establishes that the person attempting to vote corresponds to the registered voter. Privacy-preserving cryptography can then reduce the amount of sensitive information that must be exposed during later verification. Blockchain can provide the transaction layer without requiring the public ledger to contain the voter's private biometric information.

The project therefore treats facial recognition, zero-knowledge cryptography, and blockchain as complementary security mechanisms. They address different risks and should not be presented as interchangeable technologies.

XIII. OVERALL WORKFLOW

The complete workflow begins with voter registration and face enrollment. The voter subsequently logs in and enters the required voter identifier. The camera-based verification stage performs face detection, single-person checking, liveness detection, and face matching. After successful verification, the system displays the election and candidates.

The voter selects a candidate and submits the vote. The backend checks voting status and processes the ballot. The transaction-recording layer stores the voting transaction according to the blockchain-oriented design. The results module then counts the accepted votes and provides candidate-wise election information to the administrator.

This workflow connects the user interface, AI verification, backend services, database, blockchain, privacy layer, and result generation into one system. The modular organization also makes it possible to improve one component without redesigning the complete application.

ACKNOWLEDGMENT

The authors acknowledge the guidance and technical support provided by Prof. Sariya Anjum, Assistant Professor, Department of Computer Science & Engineering, Mysuru Royal Institute of Technology, Mandya, Karnataka, India, during the development of this project.

REFERENCES

[1] X. Yang, X. Yi, S. Nepal, A. Kelarev, and F. Han,

"Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," *Future Generation Computer Systems*, vol. 112, pp. 859–874, 2020. ScienceDirect

[2] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, X. Du, and M. Guizani, "A Blockchain-Based Self-Tallying Voting Protocol in Decentralized IoT," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 1, pp. 119–130, 2022. IEEE

[3] V. Sathya Preiya *et al*., "Blockchain-Based E-Voting System with Face Recognition," 2023. Fusion: Practice and Applications

[4] H. Mittal and N. Sengar, "A Blockchain and Face Recognition Based E-Voting System," *International Journal for Research in Applied Science & Engineering Technology*, vol. 13, no. 4, 2025. IJRASET

[5] S. Paudel, A. Poudel, and S. Paudel, "Enhancing Electoral Integrity and Accessibility: A Blockchain and Facial Recognition-Based Electronic Voting System," *Information Dynamics and Applications*, vol. 4, no. 2, 2025. Information Dynamics and Applications

[6] InsightFace, "InsightFace: 2D and 3D Face Analysis Project," project documentation. InsightFace

[7] Ethereum Foundation, "Ethereum Documentation," developer documentation. Ethereum

[8] Circom and snarkJS documentation, zero-knowledge circuit construction and proof-generation resources. Circom