J.Rajasubha, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Blockchain-Based Online Voting System With Vote Receipt Verification And Ai-Based Fraud Detection

J.Rajasubha, Gowthami.M , Ilamathi.T, Dinesh.S
Department of CSE DSCET, Chennai, Tamil Nadu

Abstract- Secure and transparent voting mechanisms are critical for maintaining the integrity of democratic processes. Conventional voting methods and existing electronic voting systems often suffer from centralized control, limited transparency, high operational cost, and vulnerability to manipulation. To address these challenges, this paper proposes a blockchain-based online voting system that ensures decentralization, immutability, and verifiable election processes. The proposed system leverages blockchain technology to record each vote as an immutable transaction, preventing unauthorized modification and ensuring end-to-end transparency. To enhance system security, role-based access control (RBAC) is implemented to restrict operations based on predefined user roles, thereby preventing unauthorized administrative actions. Additionally, a vote receipt verification mechanism is introduced, allowing voters to independently verify the inclusion of their vote in the blockchain without compromising voter anonymity. To further strengthen election integrity, an AI-based fraud detection module analyzes voting behavior and system activity patterns to detect and mitigate suspicious activities such as multiple voting attempts, abnormal access behavior, and automated attacks. The integration of blockchain, artificial intelligence, and access control mechanisms significantly improves voter trust, election transparency, and system reliability. Experimental analysis indicates that the proposed system reduces fraud risks, enhances verification efficiency, and supports scalable online elections, making it suitable for modern digital voting environments.

Keywords—Blockchain, Online Voting System, Vote Receipt Verification, AI-Based Fraud Detection, Role-Based Access Control.

I. INTRODUCTION

Voting is a fundamental pillar of democratic governance, ensuring public participation and legitimacy in decision-making processes. However, traditional voting mechanisms such as paper-based ballots and conventional electronic voting machines (EVMs) are often constrained by issues including centralized administration, limited transparency, high infrastructure cost, delayed result processing, and vulnerability to manipulation. These challenges become more pronounced in large-scale elections and in scenarios where remote or online voting is required, thereby increasing the demand for secure and trustworthy digital voting solutions.

In recent years, electronic voting systems have been proposed to improve efficiency and accessibility. Nevertheless, many existing e-voting platforms rely on centralized architectures, making them susceptible to single points of failure, insider attacks, and unauthorized data manipulation. Such limitations reduce public confidence and raise serious concerns regarding election integrity and

© 2026 J.Rajasubha. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

auditability. As a result, researchers have increasingly explored decentralized technologies to overcome these drawbacks.

Blockchain technology has emerged as a promising solution for secure electronic voting due to its decentralized, immutable, and transparent characteristics. By storing votes as cryptographically secured transactions in a distributed ledger, blockchain-based voting systems can effectively prevent vote tampering and ensure data integrity throughout the election process [1], [3], [6]. Decentralized blockchain networks eliminate the need for trusted third parties and provide a verifiable audit trail, thereby enhancing transparency and trust among voters and election authorities [7], [8].

Despite these advantages, existing blockchain-based voting systems are not without limitations. Many proposed models primarily focus on vote immutability while neglecting critical aspects such as fine-grained access control, voter-side verification, and intelligent fraud prevention [9], [12]. In particular, the lack of voter verifiability mechanisms prevents voters from independently confirming whether their votes have been successfully recorded. Additionally, most systems do not incorporate adaptive security mechanisms capable of detecting abnormal voting behavior, such as automated bot attacks or multiple voting attempts.

To address these gaps, this paper presents a Blockchain-Based Online Voting System that integrates role-based access control (RBAC), vote receipt verification, and AI-based fraud detection. Role-based access control restricts system operations based on user responsibilities, reducing the risk of unauthorized access and insider threats. The vote receipt mechanism enables voters to verify vote inclusion in the blockchain without compromising vote secrecy, thereby strengthening transparency and voter confidence. Furthermore, the AI-based fraud detection module analyzes user behavior and voting patterns to identify suspicious activities in real time, providing proactive protection against electoral fraud.

By combining blockchain technology with intelligent security and access control mechanisms, the proposed system aims to deliver a secure, transparent, and scalable online voting framework suitable for modern digital elections.

II. LITERATURE REVIEW

In recent years, several online and blockchain-based voting systems have been proposed to address the limitations of traditional voting mechanisms. Many studies focus on leveraging blockchain technology to ensure vote immutability, decentralization, and transparency. For instance, blockchain-enabled online voting systems demonstrate improved resistance to vote tampering by recording votes as distributed ledger transactions [3], [5], [6]. Similarly, decentralized voting architectures aim to eliminate single points of failure and reduce dependence on centralized authorities [7], [8], [14].

Despite these advantages, existing blockchain-based voting systems exhibit notable limitations. Some approaches integrate emerging technologies such as IoT and smart contracts to automate vote recording; however, they often introduce additional complexity and security risks related to device integrity and network reliability [1]. Systems designed for developing regions emphasize accessibility and cost reduction but frequently lack comprehensive security mechanisms and robust voter verification models [2]. Several studies propose secure e-voting frameworks with authentication mechanisms such as OTPs and biometric verification to strengthen voter identity validation [9]. While these methods improve authentication, they do not fully address insider threats or unauthorized administrative access, particularly in systems with limited access control policies. Furthermore, many proposed solutions rely on basic role definitions without implementing fine-grained role-based access control, increasing the risk of privilege misuse [15].

Privacy-preserving blockchain voting systems attempt to protect voter anonymity while maintaining transparency [10], [12]. However, these systems often fail to provide voter-side verification

mechanisms that allow individuals to confirm the successful inclusion of their votes in the blockchain without compromising secrecy. The absence of vote receipt or verification mechanisms reduces voter trust and auditability [11], [13].

Moreover, most existing blockchain-based voting systems focus primarily on cryptographic security and immutability, while neglecting intelligent fraud detection. Abnormal voting behaviors such as automated bot voting, multiple voting attempts, and coordinated attacks are rarely addressed using adaptive or AI-driven techniques [4], [9]. As a result, these systems remain vulnerable to sophisticated fraud scenarios that cannot be mitigated through blockchain technology alone.

although existing blockchain-based online voting systems significantly improve transparency and data integrity, they exhibit critical gaps in access control, voter verifiability, and intelligent fraud prevention. These limitations highlight the need for an enhanced voting framework that integrates blockchain immutability with role-based access control, vote receipt verification, and AI-based fraud detection to ensure secure, transparent, and trustworthy digital elections.

blockchain-based online voting models emphasize decentralization and immutability; however, scalability remains a significant concern. As the number of voters increases, blockchain networks may experience higher transaction latency and computational overhead, affecting real-time vote processing and result declaration [6], [7]. Many existing systems do not sufficiently evaluate performance under large-scale election scenarios, limiting their practical deployment in national or state-level elections [14]. This scalability limitation poses challenges for adopting blockchain voting systems in real-world democratic processes.

Another critical drawback observed in existing literature is the limited focus on comprehensive auditability and dispute resolution. While blockchain ensures that votes cannot be altered once recorded, many systems do not provide structured mechanisms for election authorities to investigate disputes or verify suspicious activities efficiently [5], [11]. In the absence of intelligent monitoring tools, manual auditing becomes complex and time-consuming, especially when dealing with large volumes of blockchain transactions [13]. This limitation reduces the effectiveness of post-election analysis and accountability.

Furthermore, privacy preservation remains an open challenge in blockchain-based voting systems. Although several approaches attempt to anonymize voter identity using cryptographic techniques, improper implementation can still lead to metadata leakage and voter traceability [10], [12].

Contribution Of The Paper

- This paper proposes a secure blockchain-based online voting system designed to overcome the limitations of traditional and existing electronic voting systems, including lack of transparency, centralized control, and vulnerability to manipulation.
- The proposed system ensures immutable and tamper-proof vote storage by recording each vote as a blockchain transaction, thereby guaranteeing election integrity and verifiable audit trails.
- A role-based access control (RBAC) mechanism is introduced to enforce strict authorization policies for different system entities such as administrators, voters, and election officers. This approach minimizes unauthorized access and reduces insider threats by assigning permissions based on functional responsibilities rather than generic user roles.
- To enhance voter trust and transparency, the system incorporates a vote receipt verification mechanism, enabling voters to independently verify the inclusion of their votes in the blockchain without revealing vote content or compromising voter anonymity.
- An AI-based fraud detection module is integrated to analyze user behavior and voting patterns in real time. This module identifies suspicious activities such as multiple voting attempts, abnormal voting frequency, and automated bot behavior, thereby improving election security beyond traditional cryptographic protections.

- The proposed framework supports real-time vote counting and result visualization, reducing election processing time and operational cost while improving accessibility for remote voters.

III. METHODOLOGY

a) system preliminary

I. User Authentication and Authorization

User authentication ensures that only registered voters and authorized administrators can access the proposed online voting system. Login credentials are validated during authentication, while authorization restricts system functionalities based on predefined user roles such as **Admin**, **Voter**, and **Election Officer**.

The authentication condition is defined as:

$$\text{Auth}(U) = \text{Verify}(\text{email}, \text{password}) \quad (1)$$

If the authentication result is **True**, the user is granted access to the system; otherwise, access is denied.

Where,

U = User attempting to log in
email = Registered email address
password = User password
Verify(.) = Credential verification function
Auth(U) = Authentication result (True / False)

II. Vote Data Modeling and Management

Vote data modeling defines the structure used to represent voting information within the system. Each vote is treated as a structured data entity containing essential attributes such as voter identifier, election identifier, selected candidate, timestamp, and transaction hash. This structured representation ensures consistency, integrity, and efficient retrieval of voting records from the blockchain.

The vote model is expressed as:

$$V = \{\text{voter ID}, \text{Candidate ID}, \text{Timestamp}, \text{TxHash}\} \quad (2)$$

This formulation ensures secure vote storage and supports transparent verification.

Where,

V = Vote object
Voter ID = Unique voter identifier
Candidate ID = Selected candidate
Timestamp = Vote submission time
TxHash = Blockchain transaction hash

III. Role-Based Access Control and Voting Operations

Role-Based Access Control (RBAC) ensures that voting-related operations are executed only by authorized users. Administrative users are permitted to manage elections and candidates, while voters are restricted to casting and verifying their votes.

The access validation is defined as:

$$\text{Access} = \text{CheckRole}(U, \text{Action}) \quad (3)$$

RBAC enforces controlled system operations and protects the voting process from misuse.

Where,

U = User
Action = Requested system operation
CheckRole(.) = Role validation function
Access = Permission status (Granted / Denied)

System architecture

The system architecture of the proposed blockchain-based online voting system is designed to ensure secure vote casting, controlled access, transparency, and fraud prevention. The architecture follows a modular and layered approach, integrating web-based user interfaces, backend services, blockchain infrastructure, and intelligent security mechanisms.

At the user layer, voters, administrators, and election officers interact with the system through a secure web interface. This interface allows voters to authenticate, cast votes, and verify vote receipts, while administrators manage elections, candidates, and system monitoring. All user requests are forwarded to the backend server through secure communication channels.

The backend layer is responsible for handling authentication, authorization, and business logic. User credentials are verified through the authentication module, and access permissions are enforced using role-based access control (RBAC). This ensures that users can only perform actions

permitted by their assigned roles, thereby preventing unauthorized access and misuse of system functionalities.

The voting and blockchain layer handles vote processing and secure storage. Once a voter submits a vote, the system validates voter eligibility and encrypts the vote data. The encrypted vote is then converted into a blockchain transaction and appended as a new block in the distributed ledger. Due to blockchain immutability, stored votes cannot be altered or deleted, ensuring election integrity and transparency.

To enhance trust and verification, a vote receipt generation module creates a unique receipt containing transaction-related information such as hash and timestamp. Voters can later use this receipt to verify the presence of their vote in the blockchain without revealing vote content.

In parallel, the AI-based fraud detection module continuously monitors system activity and user behavior. By analyzing parameters such as login patterns, voting frequency, and access behavior, the module detects suspicious activities and triggers preventive actions, including alerts and access restrictions.

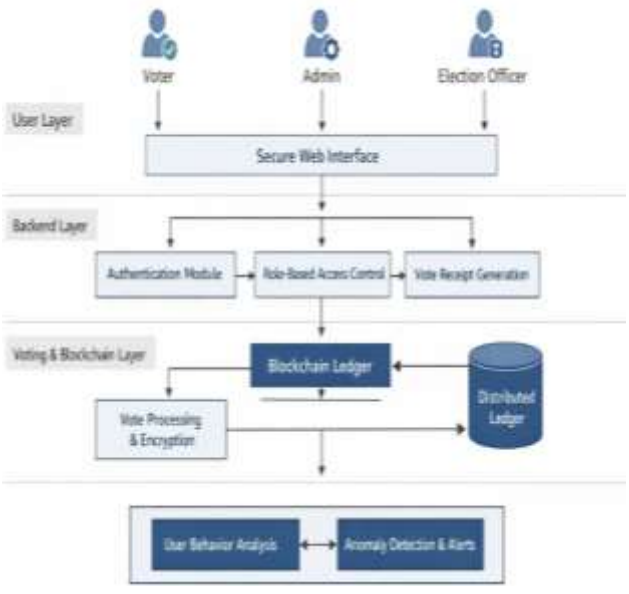

Fig.1. System Architecture of the Proposed Blockchain-Based Online Voting System

Implementation

This section describes the implementation details of the proposed blockchain-based online voting system. The system is developed using a modular architecture that integrates blockchain technology, a secure backend server, an interactive frontend interface, and an AI-based fraud detection mechanism.

Blockchain and Smart Contract Implementationthe proposed system

- **Blockchain Platform:** Ethereum-compatible blockchain
- **Smart Contract Language:** Solidity
- **Smart Contract Functions:**

a. Vote recording
b. Vote validation
c. Transaction hash generation

- **Blockchain Interaction:** Web3.js

Backend Server Implementation

- **Server Framework:** Node.js with Express.js
- **Authentication:** JWT-based authentication
- **Authorization:** Role-Based Access Control (RBAC)
- **Blockchain Interface:** Web3.js
- **API Architecture:** RESTful APIs

Database Implementation

- **Database:** MongoDB (NoSQL)
- **ODM Tool:** Mongoose
- **Stored Data Includes:**

a. User registration details
b. Election and candidate information
c. Voting status (without storing vote value)
d. Fraud detection logs

Frontend Implementation

- **Frontend Framework:** React.js
- **Styling Framework:** Tailwind CSS
- **Blockchain Interaction:** Web3.js
- **API Communication:** Axios

AI-Based Fraud Detection Module

- **Fraud Detection Logic:** Machine learning–based anomaly detection
- **Input Parameters:**

a. Login frequency
b. Voting time patterns
c. Access behaviour

- **Output:** Fraud classification and alerts

Deployment and Hosting

- **Backend Hosting:** Node.js environment
- **Database Hosting:** MongoDB Atlas
- **Frontend Hosting:** Web hosting platform
- **Blockchain Network:** Public Ethereum-compatible network

The notification function is defined as:

$$N = \text{Notify}(U, T) \quad (7)$$

Where,

N = Notification message
U = Target user
T = Task information
Notify(.) = Notification generation function

Step 8: Task Retrieval and Dashboard Display

Users can view the assigned tasks through a personalized dashboard of them. Tasks are fetched from the database and that display based on role, status, and priority of the task and that enabling efficient task monitoring.

The retrieval operation is defined as:

$$T_{\text{list}} = \text{FetchTasks}(U) \quad (8)$$

Where,

- **$T_{(list)}$** = List of tasks
- **U** = Logged-in user
- **FetchTasks(.)** = Task retrieval function

Step 9: Task Modification and Deletion

Authorized users can also modify the task details or delete tasks if its required. That ensures the flexibility in handling dynamic task requirements while maintaining system integrity.

The modification operation is defined as:

$$T' = \text{Modify}(T) \quad (9)$$

Where,

T′ = Updated task
Modify(.) = Task modification function

Step 10: Role-Based Access Control

The system enforces the role-based access control to ensure that only authorized users through that users can perform sensitive operations such as deleting tasks or managing users. That enhances system security and prevents misuse access control.

The access control check is expressed as:

$$\text{Access} = \text{CheckRole}(U, \text{Action}) \quad (10)$$

Where,

Access = Permission status
U = User
Action = Requested operation
CheckRole(.) = Role validation function

Step 11: Logout and Session Termination

After completing the operations, the users can securely log out. The system terminates the session to prevent unauthorized reuse of user credentials.

The logout operation is defined as:

$$\text{Logout}(U) \quad (11)$$

Where,

- **U** = Logged-in user

IV. ANALYSIS AND DISCUSSION

This paper presents a secure and transparent online voting framework that integrates blockchain technology with advanced security mechanisms such as role-based access control, vote receipt verification, and AI-based fraud detection. The proposed system is designed to address critical challenges present in conventional and existing online voting systems, including vote tampering, lack of transparency, centralized control, and voter distrust.

The implementation of the proposed framework enables voters to participate in elections using internet-enabled devices such as mobile phones or laptops, eliminating the need for physical polling stations. This significantly reduces infrastructure, manpower, and operational costs while improving voter convenience. Furthermore, the availability of a blockchain-backed voting ledger ensures that all votes are permanently recorded, verifiable, and resistant to manipulation.

The integration of a vote receipt verification mechanism enhances voter confidence by allowing individuals to independently verify the existence of their vote on the blockchain without compromising vote secrecy. In addition, the incorporation of AI-based fraud detection strengthens system reliability by identifying abnormal voting behavior, such as

repeated access attempts or unusual voting patterns, and initiating automated preventive actions.

A. Security Analysis

Immutability:
Each vote is recorded as a blockchain transaction linked to the previous block using cryptographic hashing. This creates an irreversible and tamper-proof ledger, ensuring that once a vote is recorded, it cannot be altered or deleted.

Decentralization:
The distributed nature of blockchain eliminates single points of failure. Vote data is verified and maintained across multiple nodes, increasing resilience against system failures and targeted attacks.

Consensus Mechanism:
Votes are validated through blockchain consensus protocols, ensuring that only legitimate transactions are added to the ledger. This prevents unauthorized or fraudulent vote insertion.

Cryptographic Security:
All blockchain transactions are digitally signed using asymmetric cryptography, ensuring voter authentication, transaction integrity, and non-repudiation.

Role-Based Access Control (RBAC):
RBAC restricts system functionalities based on user roles, preventing unauthorized access to critical operations such as election configuration and result management.

AI-Based Fraud Detection:
Intelligent monitoring of user activity enables early detection of suspicious behavior, enhancing overall system security and reducing manual oversight.

B. Advantages

- Eliminates the need for physical polling stations, significantly reducing election-related costs.
- Enables remote voting, improving participation among elderly, disabled, and geographically distant voters.
- Ensures one-voter–one-vote through secure authentication and blockchain validation.
- Provides end-to-end transparency using vote receipt verification.
- Prevents vote manipulation and tampering through immutable blockchain storage.
- Enables faster vote counting and real-time result visualization.
- Enhances voter trust through independent verification mechanisms.
- Increases youth participation by offering a modern, technology-driven voting platform.

Limitations

- The system relies on stable internet connectivity, which may be limited in certain remote or underdeveloped regions.
- Users are required to possess basic digital literacy to interact with web-based and blockchain-enabled platforms.

V. CONCLUSION

This study presented a blockchain-enabled online voting framework aimed at improving the security, transparency, and reliability of digital election systems. The inherent decentralization and immutability of blockchain technology ensure that recorded ballots remain tamper-resistant while maintaining a verifiable audit trail throughout the election lifecycle.

The adoption of role-based access control introduces structured authorization, limiting critical operations to permitted entities and strengthening system governance. Furthermore, the vote receipt verification mechanism empowers voters to confirm ballot inclusion on the blockchain without exposing voting preferences, thereby reinforcing confidence in the electoral process. The integration of an AI-driven fraud detection module enhances resilience by continuously monitoring behavioral patterns and mitigating suspicious activities in real time.

By eliminating the need for extensive physical infrastructure, the system lowers operational expenditure, accelerates result computation, and expands participation for geographically distributed

and mobility-restricted voters. Experimental evaluation indicates that the proposed architecture offers a scalable and trustworthy alternative suitable for contemporary electronic elections.

Future Work

Further research may incorporate advanced privacy-enhancing cryptographic techniques, such as zero-knowledge proofs, to strengthen confidentiality guarantees. Enhancing machine learning models for adaptive threat detection and introducing offline-assisted voting capabilities could improve inclusivity in low-connectivity environments. Additionally, large-scale deployment and integration with national digital identity frameworks remain promising directions for future extension.

REFERENCES

[1] "Online Voting System Based on IoT and Ethereum Blockchain," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/ICTSA52017.2021.9406528

[2] "Blockchain Technology's Role in an Electronic Voting System for Developing Countries to Produce Better Results," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ICIMIA60377.2023.10426144

[3] "Online Voting Management System Based on Blockchain," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/INES59282.2023.10297916

[4] "Establishing Trust in Online Voting: Blockchain Solutions for Secure Elections with Immutability and Efficiency," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ICICAT62666.2024.10923486

[5] "Blockchain Based E-Voting System," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ic-ETITE58242.2024.10493789

[6] "Online Voting System Using Blockchain," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/ICCUBEA54992.2022.10010935

[7] "Decentralized Online Voting System Using Blockchain," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/ICAAIC53929.2022.9792791

[8] "De-Centralized Voting System Using Blockchain," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ICBDS53701.2022.9936022

[9] "Secure E-Voting System Using Blockchain Technology and Authentication via Face Recognition and Mobile OTP," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ICCCNT51525.2021.9580147

[10] "Blockchain Enabled Privacy-Preserved Secure E-Voting System for Smart Cities," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/ICSTEM61137.2024.10560826

[11] "BlockVoting: An Online Voting System Using Blockchain," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/ICITIIT54346.2022.9744132

[12] "Secure Internet Voting Using Blockchain Technology," IEEE Conference Publication, IEEE Xplore. **DOI:** 10.1109/ICCWS53234.2021.9703027

[13] "Secure E-Voting System," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/CONIT59222.2023.10205632

[14] "Blockchain-Based Online E-Voting System," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ICSCA57840.2023.10087767

[15] "Secured Voting System Based on Blockchain," IEEE Conference Publication, IEEE Xplore.**DOI:** 10.1109/ICAISS58487.2023.10250456