International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

AI-Enhanced Privacy Preserving Blockchain Voting System with Zero Knowledge Verification and Off-Chain Storage

Mrs. B Dheepa[1], Mr. G. A. John Bellarmine[2]

[1]Assistant Professor, Dept. of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudur, India
[2]UG Scholar, Dept. of Information Technology Sri Venkateswara College of Engineering, Sriperumbudur, India

Abstract
Electronic voting systems have gained significant attention as an alternative to traditional paper-based elections due to their potential to improve efficiency, accessibility, and transparency. However, existing e-voting and blockchain-based voting systems primarily focus on immutability and decentralization while facing critical limitations such as inadequate voter privacy, lack of intelligent fraud detection, and poor scalability when handling large volumes of voting data. To address these challenges, this paper proposes an Artificial Intelligence (AI) enhanced privacy-preserving blockchain voting framework that integrates Zero-Knowledge Proofs (ZKP), Interplanetary File System (IPFS)-based off-chain storage, and machine learning-driven anomaly detection. In the proposed system, blockchain smart contracts are used to enforce election rules and store vote transaction hashes, while encrypted votes are stored off-chain using IPFS to reduce computational overhead. ZKP enables secure vote validation without revealing voter choices, thereby ensuring confidentiality. Additionally, an AI-based anomaly detection model, implemented using Isolation Forest and further evaluated using supervised learning models, identifies suspicious voting patterns such as bot activity, vote flooding, and coordinated attacks in real time. Experimental evaluation demonstrates that the framework achieves an anomaly detection accuracy of 80.92% using Isolation Forest, while supervised models such as Random Forest and Logistic Regression achieve accuracies of 99.63% and 99.07%, respectively, highlighting the effectiveness of hybrid detection approaches. Furthermore, the use of IPFS reduces on-chain storage requirements by approximately 70%, and the overall system maintains an average processing time of around 5 seconds per vote. The integration of these components results in a robust, scalable, and privacy-preserving voting framework that significantly improves upon existing blockchain-based solutions, making it suitable for large-scale real-world electoral applications.

Keywords: Blockchain voting; Zero-Knowledge Proof; IPFS; Anomaly Detection; Electronic Voting Security; Privacy Preservation

1. Introduction

Voting is a fundamental pillar of democratic societies, enabling citizens to express their opinions and participate in governance. Traditional voting systems, particularly paper-based elections, have been

widely adopted due to their simplicity and reliability. However, these systems are often associated with challenges such as high operational costs, time-consuming vote counting processes, susceptibility to human errors, and potential risks of manipulation. With the advancement of digital technologies, electronic voting (e-voting) systems have emerged as a promising alternative, offering improved efficiency, faster result computation, and enhanced accessibility. In recent years, blockchain technology has gained significant attention in this domain due to its decentralized, immutable, and transparent nature, making it a suitable candidate for building secure and verifiable voting systems.

Despite these advancements, existing e-voting and blockchain-based voting systems face several critical limitations. Many current implementations primarily focus on ensuring data integrity and transparency while overlooking essential aspects such as voter privacy, real-time threat detection, and scalability. Centralized e-voting systems remain vulnerable to cyber-attacks, data breaches, and unauthorized access, raising concerns about trust and reliability. Similarly, blockchain-based voting solutions often store all voting data on-chain, leading to increased computational overhead and reduced performance when handling large-scale elections. Furthermore, most existing systems lack intelligent mechanisms to detect malicious activities such as bot voting, coordinated attacks, and vote flooding, which pose serious threats to the integrity of electoral processes in real-world scenarios.

To address these challenges, this research proposes an AI-enhanced privacy-preserving blockchain voting framework that integrates multiple advanced technologies into a unified architecture. The architecture utilizes blockchain smart contracts to enforce election rules and ensure transparency, while Zero-Knowledge Proofs (ZKP) enable secure vote verification without revealing voter choices, thereby preserving privacy. Additionally, encrypted votes are stored using the Interplanetary File System (IPFS) to improve scalability by reducing on-chain storage requirements. An artificial intelligence-based anomaly detection model is incorporated to monitor voting behaviour and identify suspicious patterns in real time. By combining these components, the proposed approach aims to deliver a secure, scalable, and intelligent voting system capable of overcoming the limitations of existing solutions and supporting large-scale, real-world electoral applications.

2. Literature Review

Electronic voting systems have emerged as a promising alternative to conventional paper-based election processes due to their potential to improve accessibility, efficiency, transparency, and faster vote counting. However, traditional electronic voting systems remain vulnerable to security threats such as vote tampering, unauthorized access, identity fraud, and the absence of transparent auditing mechanisms. These limitations have encouraged researchers to investigate blockchain technology as a secure and decentralized platform for modern electoral systems [1–3].

Blockchain technology provides immutability, decentralization, transparency, and tamper resistance, making it highly suitable for secure election management. McCorry et al. proposed an Ethereum-based voting framework utilizing smart contracts to ensure transparent and publicly verifiable election results [1]. Similarly, Ben Ayed introduced a conceptual blockchain-based electronic voting protocol that enhances election integrity by eliminating centralized control [2]. Hardwick et al. further demonstrated the applicability of blockchain technology for secure electronic voting by integrating distributed ledger technology into the electoral process [3]. Although these approaches significantly improve transparency and integrity, they still face challenges related to voter privacy, storage overhead, and system scalability.

To enhance voter authentication and strengthen election security, recent blockchain-based voting systems

have incorporated biometric verification techniques. Steven et al. developed a blockchain-enabled electronic voting system utilizing the Internet Computer Protocol (ICP) together with facial recognition technology to improve voter verification and strengthen trust in electoral processes [8]. While biometric authentication effectively reduces identity impersonation and duplicate voting, these approaches provide limited support for preserving voter anonymity and detecting sophisticated cyber threats during the election process.

Privacy preservation has become another critical research focus in blockchain-enabled voting systems. Zero-Knowledge Proofs (ZKPs) have emerged as an effective cryptographic mechanism that enables voters to prove the validity of their votes without revealing the actual voting choices. Ben-Sasson et al. introduced scalable Zero-Knowledge Proof techniques that significantly improve cryptographic privacy while maintaining computational efficiency [4]. Building upon these concepts, Kumar et al. proposed a blockchain-based voting framework integrating Hyperledger Fabric, biometric authentication, and Zero-Knowledge Proofs to enhance confidentiality, transparency, and election security [9]. Despite these improvements, existing solutions primarily focus on privacy preservation and secure authentication without incorporating intelligent mechanisms capable of proactively detecting malicious voting activities.

Scalability continues to be one of the major challenges limiting the widespread adoption of blockchain-based electronic voting systems. As the number of voters increases, storing complete voting records directly on the blockchain results in higher storage requirements, increased transaction latency, and greater computational overhead. Comprehensive survey studies conducted by Jafar et al. and Ohize et al. identified scalability, storage efficiency, privacy preservation, and interoperability as significant research challenges requiring further investigation for large-scale electoral deployments [5,7].

Beyond privacy and scalability, protecting electronic voting systems against sophisticated cyber threats has become increasingly important. Artificial Intelligence and Machine Learning techniques have demonstrated significant potential for identifying anomalous patterns, malicious transactions, coordinated attacks, and abnormal user behaviour within distributed systems. Prajwalasimha proposed an AI-driven privacy-preserving cybersecurity framework that combines blockchain technology with intelligent threat detection to strengthen system security against advanced cyber-attacks [10]. Nevertheless, the integration of Artificial Intelligence into blockchain-based electronic voting systems remains relatively unexplored, with most existing voting frameworks lacking intelligent real-time fraud detection capabilities.

Furthermore, comprehensive surveys on blockchain-enabled electronic voting systems have emphasized that future research should simultaneously address privacy preservation, scalability, security, transparency, and trust through the integration of advanced cryptographic techniques and intelligent monitoring mechanisms [5,7]. Although significant progress has been achieved in individual areas such as blockchain security, biometric authentication, and Zero-Knowledge Proofs, existing solutions generally address these challenges independently rather than providing a unified framework capable of delivering comprehensive election security.

Therefore, a significant research gap exists in developing an integrated electronic voting framework that simultaneously ensures secure vote validation, voter privacy, storage scalability, transparent auditing, and intelligent fraud detection. To address this limitation, the proposed AI-Enhanced Privacy-Preserving Blockchain Voting System integrates blockchain smart contracts, Zero-Knowledge Proof-based vote verification, off-chain storage using the Interplanetary File System (IPFS), and AI-driven anomaly detection to provide a secure, scalable, transparent, and privacy-preserving solution suitable for large-scale electronic voting environments.

2.1 Research Gap and Motivation

Existing electronic and blockchain-based voting systems primarily focus on ensuring transparency, immutability, and decentralized vote storage. While these features enhance trust and data integrity, several critical challenges remain unaddressed. Most current systems lack robust mechanisms for preserving voter privacy during vote verification, often exposing sensitive information or relying on limited anonymization techniques. Additionally, scalability remains a significant concern, as storing large volumes of voting data directly on the blockchain leads to increased computational overhead, higher transaction costs, and reduced system efficiency. Another major limitation is the absence of intelligent security mechanisms capable of detecting malicious voting behaviour such as bot activity, coordinated attacks, and vote flooding in real time. These shortcomings highlight a clear research gap in developing a comprehensive voting framework that simultaneously ensures privacy, scalability, and proactive threat detection.

To address these challenges, this research proposes an integrated blockchain-based voting framework that combines advanced cryptographic techniques, scalable storage solutions, and intelligent monitoring mechanisms. The voting platform utilizes Zero-Knowledge Proofs (ZKP) to enable privacy-preserving vote verification without revealing voter choices, thereby ensuring confidentiality. To overcome scalability issues, encrypted votes are stored off-chain using the Interplanetary File System (IPFS), while only their corresponding hashes are maintained on the blockchain for integrity verification. Furthermore, an artificial intelligence-based anomaly detection model is incorporated to monitor voting patterns and identify suspicious activities in real time. This hybrid approach effectively bridges the identified research gap by providing a secure, scalable, and intelligent voting system suitable for large-scale real-world deployments.

2.2 Novel Contributions

The developed model has the following features that make it novel:

1. A decentralized voting framework is developed using blockchain smart contracts to ensure transparency, immutability, and tamper-proof vote recording without reliance on a central authority.
2. The system incorporates ZKP mechanisms to verify the validity of votes without disclosing voter identity or vote content, significantly enhancing confidentiality.
3. A machine learning model based on anomaly detection is implemented to identify suspicious voting patterns such as bot attacks, vote flooding, and coordinated manipulation attempts in real time.
4. Encrypted votes are stored in IPFS, reducing blockchain storage overhead and improving system performance while maintaining data integrity through hash references.
5. The proposed system combines AI validation, encryption, off-chain storage, and blockchain recording into a unified workflow, ensuring secure and efficient vote processing.
6. The system is evaluated using metrics such as anomaly detection accuracy, storage efficiency, and system latency, demonstrating improved performance compared to existing approaches.

3. Proposed Methodology

The framework is designed as a multi-layered architecture integrating blockchain technology, cryptographic verification, off-chain storage, and artificial intelligence-based anomaly detection as depicted in Figures 1 and 2. The architecture consists of four major modules: (A) Blockchain Layer, (B) Privacy Layer, (C) Storage Layer, and (D) Intelligence Layer. These components work together to ensure secure, scalable, and privacy-preserving voting.

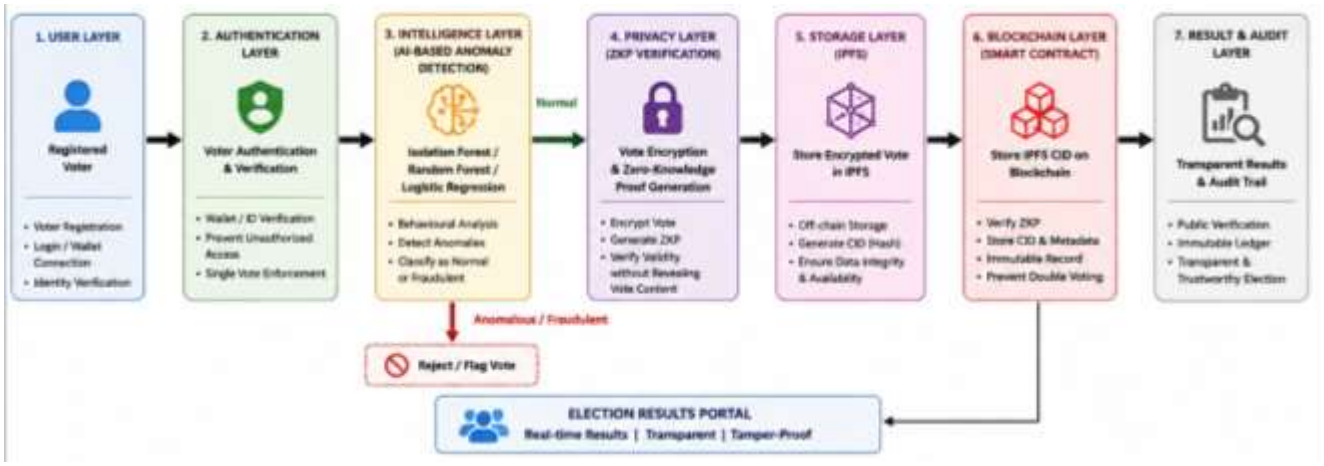


Figure 1. Architecture of Proposed Voting Framework

Figure 2. Workflow of the Proposed Voting Framework

3.1 Blockchain Layer (Smart Contract-Based Voting System)

The blockchain layer is responsible for maintaining the integrity and transparency of the voting process. It is implemented using Ethereum smart contracts that enforce election rules such as voter registration, vote casting, and prevention of double voting. Instead of storing complete vote data, only the cryptographic hash (CID) of the vote is stored on-chain, ensuring immutability while reducing storage overhead as represented in Equations (1) and (2). Let (V) represent the vote and (H(V)) denote its hash stored on the blockchain:

$$H(V) = \{Hash\}(V) \qquad (1)$$

Each vote transaction is validated using:

$$T = \{ID\_v, H(V), t\} \qquad (2)$$

Where,
(ID_v) = voter ID
(H(V)) = vote hash
(t) = timestamp.

The blockchain ensures:

- Immutability: Once recorded, votes cannot be altered.
- Transparency: All transactions are publicly verifiable.
- Security: Cryptographic hashing ensures data integrity.

3.2 Privacy Layer (Zero-Knowledge Proof-Based Verification)

To preserve voter privacy, the system employs Zero-Knowledge Proofs (ZKP), allowing verification of vote validity without revealing the actual vote content as shown in Equations (3) and (4). This ensures that sensitive voter information remains confidential while maintaining verifiability. The ZKP model can be represented as:

$$\text{Prover} -> \text{Verifier}: \text{Proof}(\text{V in ValidSet}) \quad (3)$$

$$\text{P(x)} -> \text{V}: \text{Proof}(\text{x in S}) \quad (4)$$

Where,
(x) = secret vote
(S) = set of valid votes

The system satisfies:

- **Completeness**: Valid votes are always accepted
- **Soundness**: Invalid votes are rejected
- **Zero-knowledge**: No information about the vote is revealed

This mechanism ensures secure vote validation without compromising anonymity.

3.3 Storage Layer (IPFS-Based Off-Chain Storage)

To address scalability challenges, the system utilizes the Interplanetary File System (IPFS) for storing encrypted votes off-chain. Each vote is encrypted before being uploaded to IPFS, and a unique Content Identifier (CID) is generated as shown in Equations (5) and (6). The encryption process is defined as:

$$E(V) = Enc(V, K) \quad (5)$$

Where,
(V) = vote
(K) = encryption key

The CID generated is:

$$CID = Hash(E(V)) \quad (6)$$

This provides the following advantages:

- Reduces blockchain storage load
- Ensures data availability in distributed storage
- Maintains data integrity through hash referencing

3.4 Intelligence Layer (AI-Based Anomaly Detection)

The intelligence layer incorporates machine learning techniques to detect fraudulent voting behaviour in real time. Initially, an unsupervised anomaly detection model based on the Isolation Forest algorithm is employed to identify abnormal voting patterns without prior labelling. In addition, supervised learning

models such as Random Forest and Logistic Regression are utilized for comparative evaluation and improved classification performance. The detection process is based on behavioural features extracted from voting activity as shown in Equations (7) and (8). Let the feature vector be defined as:

$$X = \{x\_1, x\_2, x\_3\} \quad (7)$$

Where,
(x_1) = Time gap between votes
(x_2) = Votes per minute
(x_3) = Same IP count

The anomaly score is computed as:

$$\text{Score}(X) = 2^{-\frac{[E(h(X))]}{[c(n)]}} \quad (8)$$

Where,
(E(h(X))) = Expected path length
(c(n)) = Normalization factor

The decision function is defined as:

$$f(x) = \begin{cases} -1, \text{if anomaly (fraudulent)} \\ 1, \text{if normal} \end{cases} \quad (9)$$

For supervised models, classification is performed using labelled data, where the output is directly mapped to normal or fraudulent classes as shown in Equation (9). The combination of unsupervised and supervised approaches enhances the robustness of the system by enabling detection of both known and unknown attack patterns. This intelligence layer ensures:

- Early detection of malicious activities
- Prevention of fraudulent votes before blockchain storage
- Improved system reliability and adaptability

3.4.1 Dataset Description

A synthetic dataset was generated to simulate both legitimate and malicious voting behaviour with overlapping feature distributions to reflect real-world conditions. The dataset includes features such as time gap between votes, voting frequency, and repeated IP activity.

- Total samples: 1800
- Normal samples: 1200
- Malicious samples: 600

The dataset was used to train and evaluate both unsupervised and supervised machine learning models.

3.4.2 Overall Workflow

The complete voting process follows these steps:

1. User initiates voting request

2. AI model evaluates voting behaviour
3. If classified as legitimate, the vote is encrypted
4. Encrypted vote is uploaded to IPFS
5. CID is generated and stored on blockchain
6. ZKP verifies vote validity without revealing content

This integrated workflow ensures:

- Security through blockchain
- Privacy through ZKP
- Scalability through IPFS
- Intelligence through AI

4. Results and Discussion

The proposed AI-enhanced blockchain voting system was evaluated based on performance, security, scalability, and anomaly detection capability. The system integrates four major components: Blockchain Layer, Privacy Layer (ZKP), Storage Layer (IPFS), and Intelligence Layer (AI model). Experimental results demonstrate the effectiveness of each module individually as well as the overall system performance.

4.1 Evaluation Metrics

The following metrics were used for evaluation:

- **Accuracy:** Measures the overall correctness of classification as in Equation (10)
- **Precision:** Indicates the proportion of correctly identified fraudulent votes as in Equation (11)
- **Recall:** Measures the ability to detect actual fraudulent votes as in Equation (12)
- **F1-Score:** Harmonic mean of precision and recall
- **Latency:** Time taken for complete vote processing
- **Storage Efficiency:** Reduction in blockchain storage usage
- **Throughput:** Number of votes processed per unit time

Mathematically:

$$\text{Accuracy} = \text{TP} + \text{TN} / \text{TP} + \text{TN} + \text{FP} + \text{FN} \quad (10)$$

$$\text{Precision} = \text{TP} / \text{TP} + \text{FP} \quad (11)$$

$$\text{Recall} = \text{TP} / \text{TP} + \text{FN} \quad (12)$$

4.2 AI-Based Anomaly Detection Results

The anomaly detection module was evaluated using a synthetic dataset consisting of 1800 samples (1200 normal and 600 malicious) with overlapping feature distributions to simulate real-world voting scenarios. Three models were evaluated: Isolation Forest (unsupervised), Random Forest, and Logistic Regression (supervised). The performance results are summarized below in Table 1.

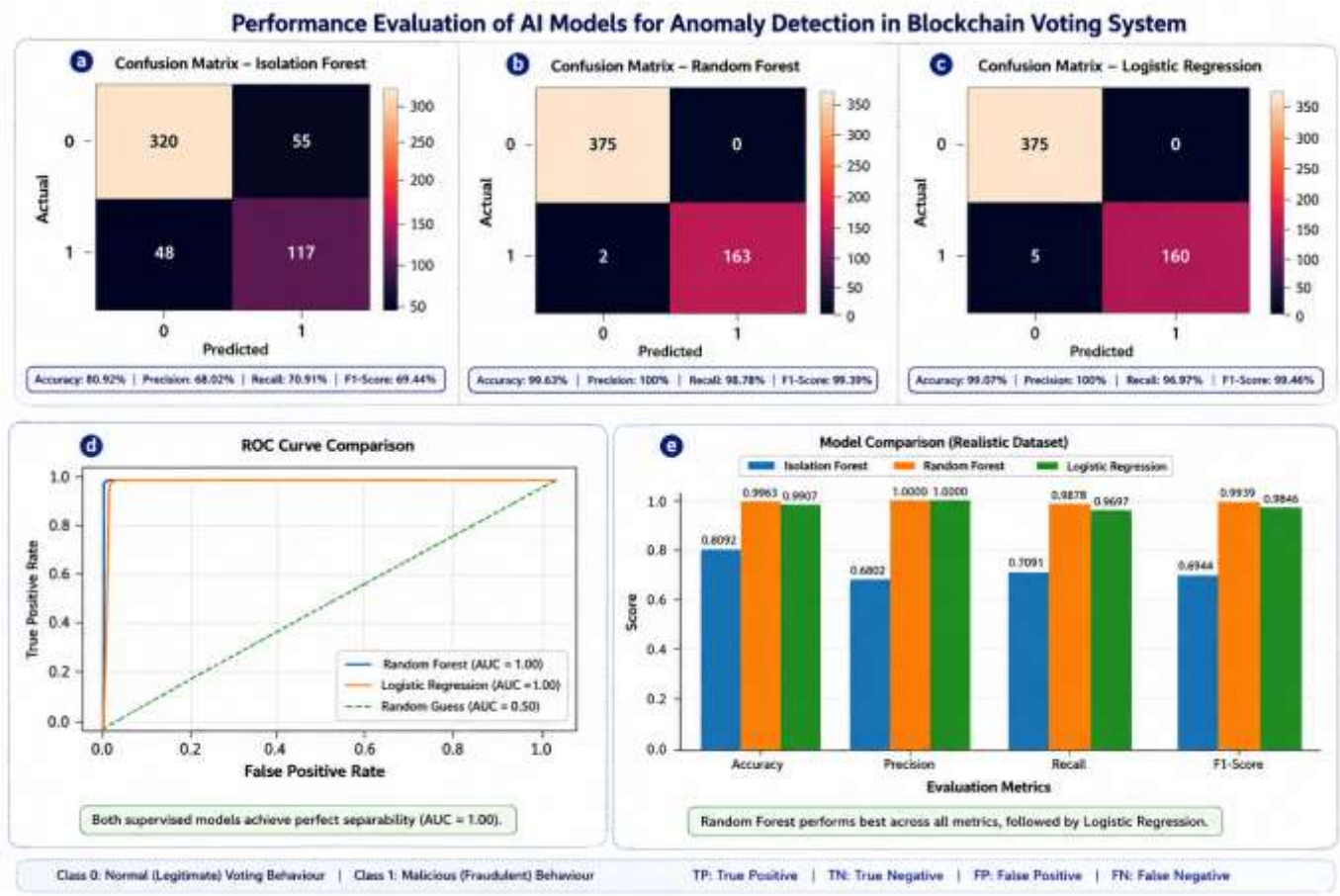
Table 1. Performance Comparison of AI Models

Model	Accuracy	Precision	Recall	F1-Score
Isolation Forest	80.92%	68.02%	70.91%	69.44%
Random Forest	99.63%	100%	98.78%	99.39%

Logistic Regression	99.07%	100%	96.97%	98.46%

Figure 3 shows that the Random Forest model achieves the highest performance across all evaluation metrics, demonstrating its effectiveness in capturing complex voting behaviour patterns. Logistic Regression also performs competitively, achieving high accuracy with slightly lower recall. In contrast, Isolation Forest exhibits comparatively lower performance due to its unsupervised nature, as it does not utilize labelled data for training. However, it remains valuable for detecting unknown or previously unseen attack patterns.

The introduction of overlapping feature distributions ensures that the evaluation reflects realistic voting conditions, preventing overly optimistic performance results. The high precision values observed in supervised models indicate a low false positive rate, while high recall values confirm the system's ability to detect most fraudulent activities. These results demonstrate the robustness of the proposed hybrid detection approach in enhancing the security of blockchain-based voting systems.



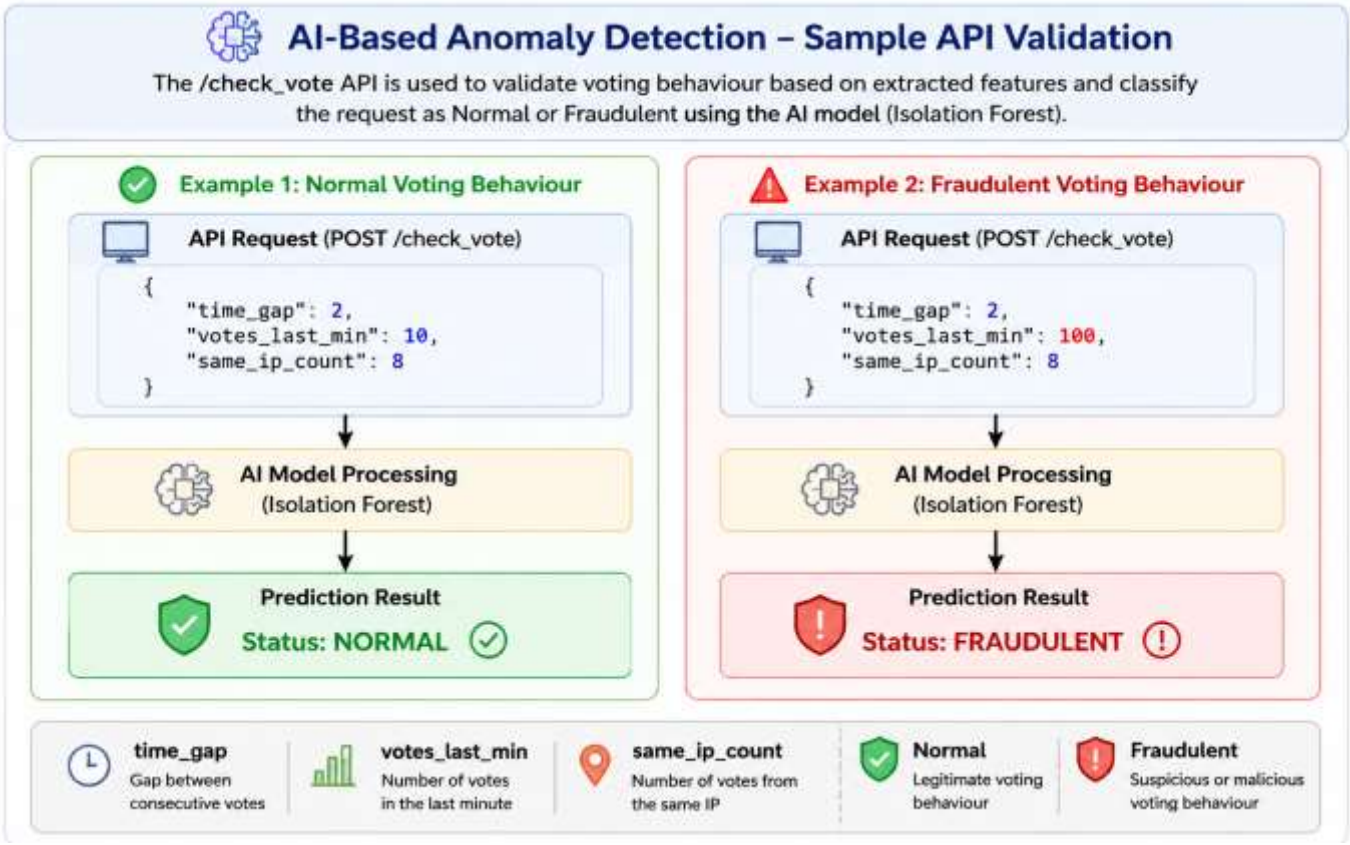


Figure 3. Performance Evaluation and AI-Based Anomaly Detection Results

4.3. Blockchain Performance Analysis

The blockchain module was evaluated based on transaction execution time and gas efficiency as tabulated in Table 2.

Table 2. Blockchain Performance Analysis

Parameter	Value
Average Transaction Time	2–4 sec
Gas Cost per Vote	Low (CID only stored)
Double Voting	Prevented

By storing only the IPFS CID instead of full vote data, the system significantly reduces gas consumption and improves transaction efficiency as shown in Figure 4. Smart contracts successfully enforce election rules, including voter authentication and prevention of duplicate voting. The immutability of blockchain ensures tamper-proof vote recording.

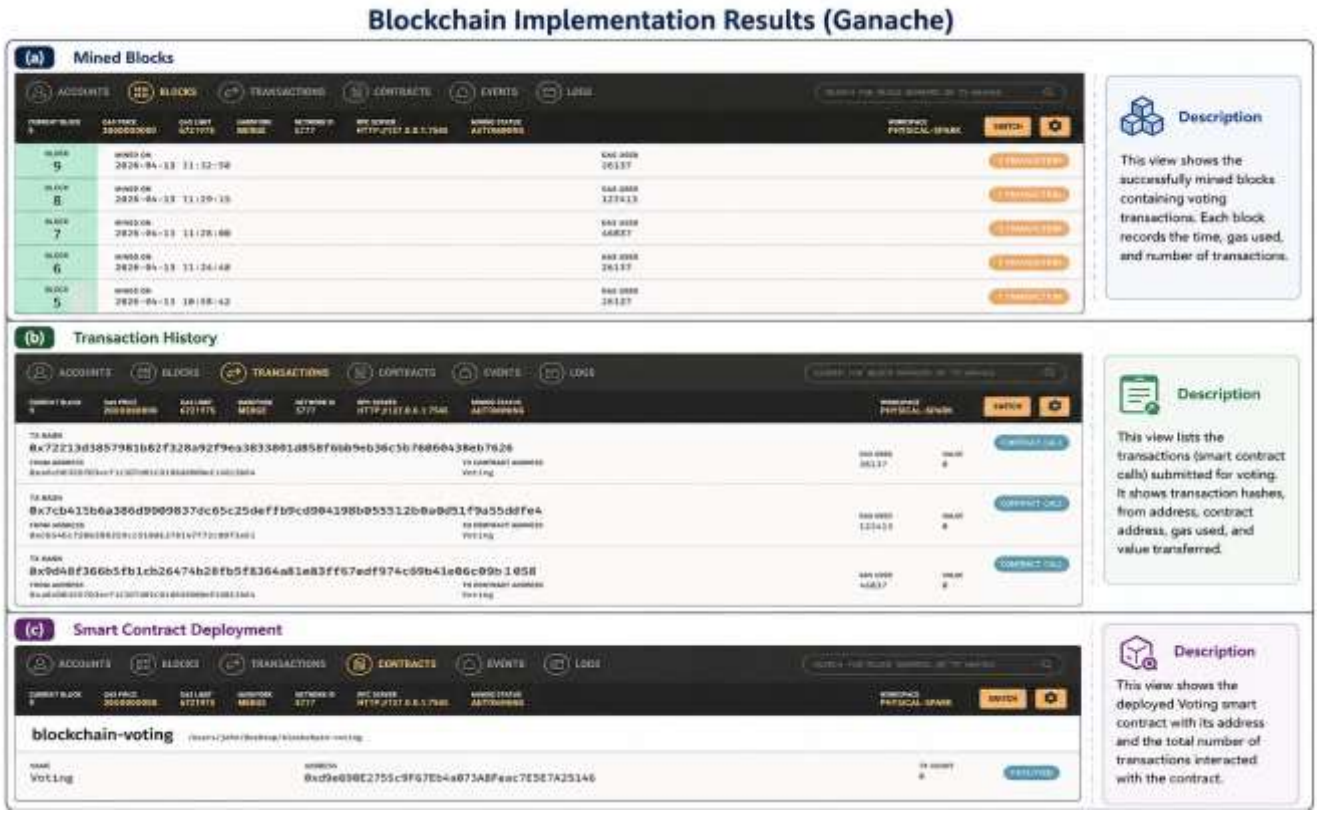


Figure 4. Blockchain Performance Analysis

4.4 IPFS Storage Performance

The storage module was evaluated based on data size and retrieval efficiency as shown in Table 3.

Table 3. IPFS Storage Performance Analysis

Parameter	Value
Storage Reduction	~70%
Upload Time	< 2 sec
Retrieval Time	~1–2 sec

Off-chain storage using IPFS significantly reduces blockchain storage overhead. Encrypted votes stored in IPFS ensure confidentiality while maintaining accessibility as depicted in Figure 5. The CID-based referencing ensures data integrity, as any modification results in a different hash. This approach improves scalability, making the system suitable for large-scale elections.

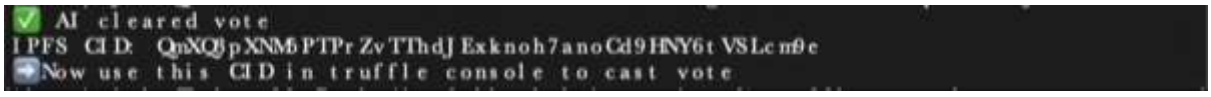


Figure 5. Off-Chain Storage using IPFS

4.5. Privacy and Security Analysis (ZKP Layer)

The Zero-Knowledge Proof mechanism was evaluated based on its ability to validate votes without revealing sensitive information.

Table 4. Privacy and Security Analysis

Property	Status
Confidentiality	Achieved
Verifiability	Achieved
Data Leakage	None

Figure 6 illustrates how ZKP ensures vote validity without exposing voter identity or vote content. This eliminates risks associated with vote tracing and enhances voter trust. The system satisfies the core principles of completeness, soundness, and zero-knowledge as summarised in Table 4, making it highly suitable for privacy-critical applications like voting.

Figure 6. Vote Validation through ZKP

4.6. End-to-End System Performance

The overall system was evaluated by integrating all modules and measuring total voting time which is shown in Table 5.

Table 5. Overall System Performance

Stage	Time
AI Validation	~0.5 sec
Encryption	~0.2 sec
IPFS Upload	~1.5 sec
Blockchain Transaction	~3 sec
Total Time per Vote	**~5 sec**

The complete voting process is executed within approximately 5 seconds per vote, which is efficient for real-world applications. The pipeline ensures that only verified and secure votes are recorded, maintaining both performance and security.

4.7. Comparative Analysis

Compared to existing systems, the proposed framework provides a more comprehensive solution by integrating privacy, scalability, and intelligent security. The hybrid approach significantly improves system robustness and practicality as shown in Table 6.

Table 6. Comparative Analysis

Feature	Existing Systems	Proposed System
Privacy Preservation	Limited	High (ZKP)
Fraud Detection	Not available	AI-based
Scalability	Low	High (IPFS)
Data Storage	On-chain	Hybrid
Security	Moderate	Enhanced

The experimental results clearly demonstrate that the developed model successfully addresses the limitations of traditional and blockchain-based voting systems. The integration of AI enables proactive fraud detection, while ZKP ensures privacy-preserving verification. IPFS reduces storage overhead and enhances scalability, and blockchain guarantees transparency and immutability.

Overall, the system achieves a balanced trade-off between security, performance, and scalability, making it a viable solution for modern electronic voting systems. The modular architecture also allows future enhancements, such as integrating advanced deep learning models or deploying on public blockchain networks.

5. Conclusion and Future Scope

The proposed AI-enhanced privacy-preserving blockchain voting system effectively addresses key limitations in existing electronic and blockchain-based voting frameworks by integrating blockchain smart contracts, Zero-Knowledge Proofs (ZKP), Interplanetary File System (IPFS), and an intelligent anomaly detection module. The system ensures a secure, transparent, scalable, and reliable voting process suitable for modern electoral requirements. Experimental evaluation on a synthetic dataset of 1800 samples demonstrates that the Isolation Forest model achieves an anomaly detection accuracy of 80.92%, while supervised models such as Random Forest and Logistic Regression achieve accuracies of 99.63% and 99.07%, respectively, with high precision and recall values. These results highlight the effectiveness of combining unsupervised and supervised approaches for robust fraud detection. Additionally, the use of IPFS reduces on-chain storage requirements by approximately 70%, significantly enhancing scalability, while maintaining an average end-to-end voting latency of around 5 seconds per vote. The blockchain layer ensures immutability and prevents double voting, whereas ZKP guarantees vote confidentiality without exposing sensitive voter information. Overall, the proposed framework provides a comprehensive and practical solution for secure and scalable electronic voting. The integration of blockchain, Zero-Knowledge Proofs, IPFS, and Artificial Intelligence into a unified framework represents the primary contribution of this work.

In future, the architecture can be extended by incorporating advanced deep learning techniques to further improve fraud detection accuracy and adapt to evolving attack patterns. Deployment on public blockchain networks or Layer-2 scaling solutions can be explored to enhance real-world applicability and reduce transaction costs. Integration of biometric authentication mechanisms, such as facial recognition or fingerprint verification, can strengthen voter identity validation. Furthermore, optimization of Zero-Knowledge Proof protocols and smart contract execution can reduce computational overhead and latency. Large-scale real-world testing using diverse and dynamic datasets can also be conducted to validate system robustness, security, and scalability under practical electoral conditions.

Acknowledgement:
The authors express their sincere gratitude to the project mentor and faculty members for their continuous guidance, valuable insights, and technical support throughout the research work. The authors also thank all team members for their dedicated contributions across various modules, including blockchain development, machine learning model implementation, IPFS integration, and system design. Their collaborative efforts were instrumental in the successful completion of this project. The authors further acknowledge the institution for providing the necessary infrastructure and resources to carry out this research effectively.

References

1. P. McCorry, S. Shahandashti, F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy", Lecture Notes in Computer Science, 2017. https://doi.org/10.1007/978-3-319-70972-7_20
2. A. Ben Ayed, "A Conceptual Secure Blockchain Based Electronic Voting System", International Journal of Network Security & Its Applications, 9, 01–09, 2017. https://doi.org/10.5121/ijnsa.2017.9301
3. F. S. Hardwick, A. Gioulis, R. N. Akram, K. Markantonakis, "E-Voting With Blockchain", Proceedings of the 2018 IEEE International Conference on Blockchain, IEEE, 2019, 1–7. https://doi.org/10.1109/Cybermatics_2018.2018.00262
4. E. Ben-Sasson, A. Chiesa, E. Tromer, M. Virza, "Scalable Zero Knowledge via Cycles of Elliptic Curves", Cryptology ePrint Archive, Paper 2014/595, 2014. https://eprint.iacr.org/2014/595
5. U. Jafar, M. Ab Aziz, Z. Shukur, H. Hussain, "A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems", Sensors, 22, 7585, 2022. https://doi.org/10.3390/s22197585
6. C. Onur, A. Yurdakul, "ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol", Distributed Ledger Technologies: Research and Practice, 2, 2023. https://doi.org/10.1145/3598302
7. H. Ohize, A. Onumanyi, B. Umar, A. Lukman, R. Isah, E. Dogo, B. Nuhu, O. Olaniyi, J. Ambafi, V. Sheidu, M. Ibrahim, "Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges", Cluster Computing, 28, 2024. https://doi.org/10.1007/s10586-024-04709-8
8. Steven, F. Hadiprodjo, I. Alam, L. Wulandhari, "Implementation of Blockchain-Based Electronic Voting System: A Case Study in Indonesia", Procedia Computer Science, 269, 1–12, 2025. https://doi.org/10.1016/j.procs.2025.08.253
9. N. Kumar, S. Kumar, A. Waqar, C. Ngantung, "Modernizing Voting Systems: A Comprehensive Approach Using Blockchain, Biometrics and Zero Knowledge Proofs", International Journal of Electrical, Computer, and Biomedical Engineering, 3, 2025. https://doi.org/10.62146/ijecbe.v3i3.116
10. S. N. Prajwalasimha, "AI-Driven Cyber Threat Intelligence with Blockchain: A Federated and Privacy-Preserving Approach (FPPA) for Secure Defense", Proceedings of the International Conference on Intelligent Systems and Computing, 2025. https://doi.org/10.1109/ICISC65841.2025.11188430