International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

Blockchain Powered E-Voting With Ai-Based Facial Recognition And Multi-Factor Authentication

Mrs. Karthica C[1],Harini S[2], Ilakkiya B[3],Iswarya S[4]
[1]Assistant professor, Dept. of CSE, Sri Manakula Vinayagar Engineering College, Puducherry, India
[2,3,4]UG Scholar, Dept. of CSE, Sri Manakula Vinayagar Engineering College, Puducherry, India
Email ID: *karthika1me@gmail.com[1], svharini1705@gmail.com[2], ilakkibala0623@gmail.com[3], iswaryasms11@gmail.com[4]*

Abstract
The integrity of democratic voting systems is increasingly threatened by security vulnerabilities, lack of transparency, and trust deficits, making electoral processes susceptible to manipulation. To address these concerns, Binance Smart Chain (BSC) introduces a blockchain-powered voting framework that leverages the Proof of Staked Authority (PoSA) consensus protocol to enhance security and decentralization. To further fortify the system, ResNet-101, a deep learning-based convolutional neural network (CNN), is integrated for facial recognition authentication, ensuring voter legitimacy and eliminating identity fraud. Additionally, one-time password (OTP) authentication and live location tracking strengthen the system against unauthorized access and proxy voting. By combining blockchain technology, biometric verification, and AI-driven facial authentication, BSC establishes a highly secure, transparent, and tamper-proof voting system. This approach aims to restore public trust in electoral processes, setting a new benchmark for secure and verifiable digital voting systems in democratic governance.
Keywords: *Blockchain, PoSA, ResNet-101, Facial Recognition, OTP, Voting Security, Transparency, Authentication.*

1. Introduction
Elections are fundamental to democratic governance, yet traditional voting mechanisms such as paper ballots and postal voting suffer from issues including ballot damage, tampering risks, high operational costs, delivery delays, and time-consuming manual counting. Even modern electronic voting systems require voters to be physically present at polling stations, which can reduce accessibility and participation. In countries such as India, postal ballots provided to service personnel and election officials often face rejection due to marking errors or logistical delays, highlighting the need for a more secure and accessible digital alternative. Consequently, this project proposes a **secure web-based remote voting system integrating Artificial Intelligence and Blockchain technology** to ensure transparency, privacy, fairness, and improved voter participation. The system incorporates **deep learning–based facial recognition using the ResNet-101 model combined with multi-factor authentication (OTP verification and live location validation)** to prevent impersonation, proxy voting, and duplicate voting. Blockchain implementation through the Binance Smart Chain using the Proof of Staked Authority (PoSA) consensus mechanism ensures decentralized architecture, tamper-proof vote storage, fast transaction validation, and transparent record maintenance.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

Additionally, smart contracts automatically enforce election rules, reducing human intervention and eliminating potential manipulation, thereby providing a secure, scalable, and trustworthy remote electronic voting framework.

2. Related Work

Research in Natural Language Processing (NLP) and Intelligent Document Processing (IDP) has significantly improved the extraction and management of knowledge from unstructured documents. NLP transforms heterogeneous text into structured, searchable information, enhancing accessibility and large-scale knowledge management. Recent advancements in Large Language Models (LLMs) and Retrieval-Augmented Generation (RAG) further enable semantic analysis, contextual summarization, and intelligent question answering, thereby reducing manual effort, minimizing errors, and accelerating document-centric workflows across industries. However, most existing solutions focus on isolated tasks such as retrieval or compliance monitoring without offering a unified framework. The proposed TransformoDocs framework addresses this gap by **integrating NLP, LLMs, and RAG pipelines into a scalable hybrid architecture** that converts unstructured documents into standardized, semantically enriched knowledge assets. It also **embeds automated compliance enforcement and accessibility support within document workflows**, ensuring improved efficiency, regulatory adherence, and comprehensive enterprise-level knowledge management.

3. Proposed System

The proposed system presents a secure, decentralized, and intelligent online voting framework by integrating blockchain technology, deep learning–based biometric authentication, and multi-factor security mechanisms. The primary objective of this system is to eliminate security vulnerabilities, identity fraud, and lack of transparency present in traditional and existing electronic voting systems. The system is built on the Binance Smart Chain (BSC) blockchain platform, which offers high transaction throughput and low latency. The Proof of Staked Authority (PoSA) consensus mechanism is utilized to ensure fast and secure validation of voting transactions. To strengthen voter authentication, the system employs ResNet-101, a deep convolutional neural network (CNN), for facial recognition. Additionally, One-Time Password (OTP) verification and live location tracking are incorporated to prevent unauthorized access and fraudulent voting. By combining blockchain immutability with AI-driven authentication, the proposed system ensures that each vote is verifiable, tamper-proof, and transparent, thereby improving public trust in the electoral process.

Proposed Architectural Diagram

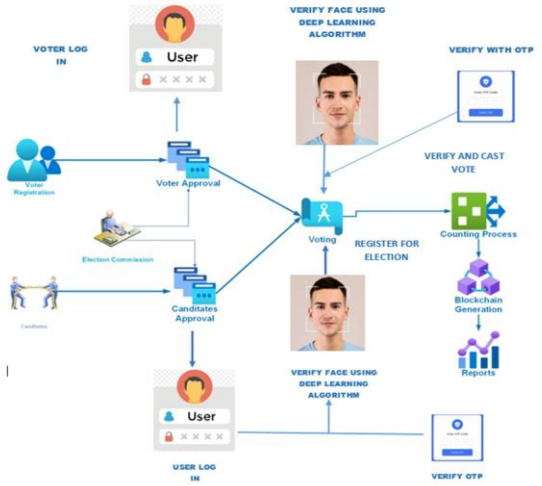


Figure 1 Architecture Diagram

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

The proposed architecture in **figure 1** begins with the voter and candidate registration module, where users submit their personal details for verification. Voters provide government-issued identification, facial biometric data, and location information, while candidates submit identity and eligibility details. These details are forwarded to the Election Commission module, which verifies and approves both voters and candidates before granting system access. Once registration is approved, voters proceed to the login module, where identity verification is performed using deep learning–based facial recognition (ResNet-101). The live facial image captured during login is matched with the stored biometric template to confirm voter authenticity. This mechanism prevents impersonation, duplicate voting, and proxy voting. To further enhance security, OTP-based authentication is implemented as an additional verification layer. The OTP is dynamically generated and sent to the voter's registered mobile number. Only users who successfully complete both facial recognition and OTP verification are allowed to access the voting interface. After authentication, voters enter the voting module, where they can select their preferred candidate. Before vote submission, the system ensures session integrity through final verification. The vote is then encrypted and submitted as a transaction. Each vote is securely recorded on the Binance Smart Chain (BSC) blockchain using the PoSA consensus protocol. Smart contracts govern the voting rules, prevent double voting, and automate vote recording and counting. Due to blockchain immutability, once a vote is recorded, it cannot be altered or deleted. Finally, the counting and reporting module retrieves voting data directly from the blockchain ledger and generates election results in real time. Since all votes are stored on a decentralized ledger, the results are transparent, auditable, and tamper-proof while maintaining voter anonymity.

3. Proposed Algorithm

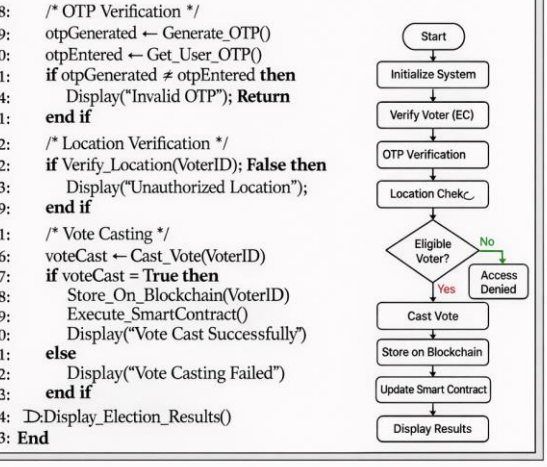
The proposed algorithm ensures a secure, authenticated, and tamper-proof e-voting process by integrating facial recognition, OTP verification, location validation, and blockchain-based vote recording. The algorithm operates in sequential phases: registration, authentication, vote casting, blockchain storage, and result generation.

Pseudocode

Algorithm 1: Blockchain-Based E-Voting System

Input: Voter credentials, facial image, OTP, location data
Output: Authenticated vote stored on Binance Smart Chain, election results

```
Begin
    · Initialize system parameters
    · Connect to Binance Smart Chain Network
    · Load Election Smart Contract
    voteCast ← False
    /* Registration Phase */
    ecApproved ← Verify_ElectionCommission(VoterID)
    if ecApproved = False then
        Display("Voter Not Approved"); Return
    end if
    /* Facial Recognition Authentication */
    faceMatch ← Verify_Facial(ResNet101, VoterID)
    if faceMatch = False then
        Display("Facial Authentication Failed"); Return
    end if
    /* OTP Verification */
    otpGenerated ← Generate_OTP()
    otpEntered ← Get_User_OTP()
    if otpGenerated ≠ otpEntered then
        Display("Invalid OTP"); Return
    end if
    /* Location Verification */
    if Verify_Location(VoterID); False then
        Display("Unauthorized Location");
    end if
    /* Vote Casting */
    voteCast ← Cast_Vote(VoterID)
    if voteCast = True then
        Store_On_Blockchain(VoterID)
        Execute_SmartContract()
        Display("Vote Cast Successfully")
    else
        Display("Vote Casting Failed")
    end if
    D:Display_Election_Results()
End
```



International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

4. Implementation and Results

Implementation

The proposed blockchain-based e-voting system was implemented by integrating ResNet-101 deep learning architecture, multi-factor authentication, and Binance Smart Chain (BSC) to ensure secure and transparent elections. The facial recognition module was implemented using ResNet-101, which consists of an initial convolutional layer, multiple residual blocks, and a global average pooling layer followed by a fully connected layer. This architecture enables robust feature extraction and high authentication accuracy while mitigating vanishing gradient issues through skip connections. The authentication framework combines facial recognition, OTP verification, and live location tracking to prevent impersonation, proxy voting, and unauthorized access. Once authentication is successful, votes are encrypted and transmitted to the blockchain network. The Proof of Staked Authority (PoSA) consensus mechanism is employed to ensure fast block validation and reduced transaction latency.

Smart contracts deployed on BSC automate vote validation, prevent double voting, securely store transactions, and perform real-time vote counting. The decentralized ledger ensures immutability and transparency, eliminating manual intervention and vote manipulation.

Results

Accuracy measures the system's ability to correctly authenticate legitimate voters while rejecting fraudulent attempts. It is computed as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Experimental results indicate that the ResNet-101-based facial recognition module achieves an accuracy exceeding 98%, significantly reducing false acceptance and false rejection rates.

The integration of OTP and location verification further enhances authentication reliability, making the system highly secure and fraud-resistant.

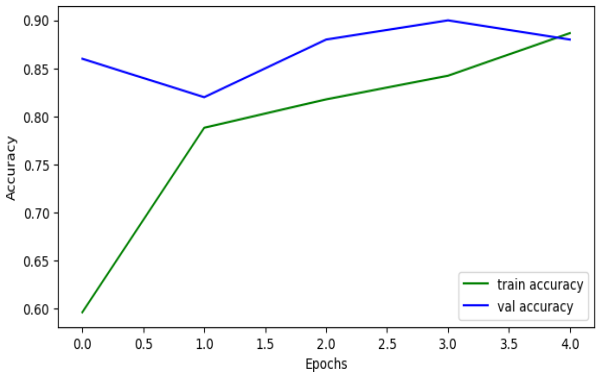


Figure 2 Training and Validation Accuracy of ResNet-101 Facial Recognition Model

Figure 2 illustrates the training and validation accuracy of the ResNet-101 facial recognition model across multiple epochs. Initially, the training accuracy starts at a lower value due to random weight initialization but gradually improves as the model learns meaningful facial features. The validation accuracy remains consistently high, demonstrating strong generalization capability and minimal overfitting.

Loss

The ResNet-101 model employs Cross-Entropy Loss, defined as:

$$\text{Loss} = -\frac{1}{N}\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

During training, the loss value decreases steadily across epochs, demonstrating effective learning

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

and convergence. Batch normalization and residual connections stabilize the loss curve, preventing overfitting and improving generalization. The smooth decline of loss confirms the robustness of the facial recognition model.

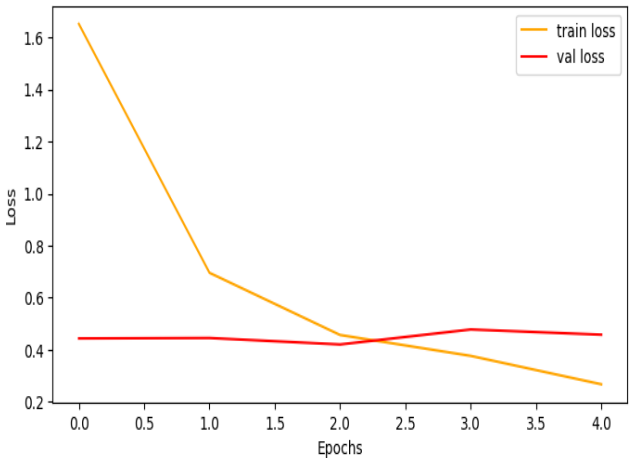


Figure 3 Training and Validation Loss of ResNet-101 Facial Recognition Model

Figure 3 presents the training and validation loss curves of the ResNet-101 model over successive epochs. The training loss shows a rapid decline, indicating efficient learning and convergence of the network. The validation loss remains relatively stable, reflecting the model's ability to generalize well to unseen data. **Table 1** presents a comparative evaluation between the traditional e-voting system and the proposed blockchain-based secure e-voting framework. The existing system primarily relies on password or ID-based authentication, which offers moderate fraud resistance and comparatively lower authentication accuracy (approximately 85–88%). In contrast, the proposed system integrates multi-factor authentication mechanisms, including facial recognition, one-time password (OTP), and location verification, thereby significantly improving authentication accuracy to above 98% and enhancing fraud resistance.

Table 1 Comparison Between Existing System and Proposed System

Metric	Existing System	Proposed System
Authentication Method	Password / ID	Face + OTP + Location
Authentication Accuracy	85–88%	>98%
Fraud Resistance	Moderate	Very High
Block Time	High	~3 seconds
Gas Fee	High	Low
Vote Storage	Centralized	Blockchain (Immutable)
Vote Counting	Manual / Semi-auto	Smart Contract Based
Scalability	Limited	High

Additionally, the traditional system uses centralized storage and manual or semi-automated vote counting processes, which may introduce delays and security vulnerabilities. The proposed system leverages blockchain technology for immutable vote storage and smart contracts for automated vote counting, ensuring transparency, integrity, and faster processing. Furthermore, the proposed approach reduces block confirmation time to approximately three seconds, lowers gas fees through optimized blockchain operations, and improves overall system scalability compared to the existing system.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

5. Performance And Analysis

To evaluate the stability, consistency, and reliability of the proposed blockchain-based e-voting system, statistical performance measures such as Mean, Variance, and Standard Deviation were computed. These metrics provide deeper insight into the behavior of the system across multiple training epochs and voting transactions.

5.1 Mean Performance

The mean (average) represents the overall performance level of the system across multiple observations. For facial recognition accuracy, the mean value indicates the average authentication accuracy achieved during training and validation. The mean is calculated as:

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i$$

where
represents the observed performance value (accuracy or loss), and
is the total number of observations.
A higher mean accuracy reflects improved voter authentication reliability, while a lower mean loss indicates better model convergence.

5.2 B. Variance

Variance measures the degree of dispersion of performance values around the mean. It indicates how much the system's performance fluctuates during training or execution.
Variance is defined as

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N} (x_i - \mu)^2$$

A low variance signifies stable and consistent performance across epochs, while high variance may indicate instability or sensitivity to input variations. In the proposed system, low variance in accuracy confirms consistent facial recognition results.

5.3 C. Standard Deviation

Standard deviation represents the square root of variance and provides a more interpretable measure of dispersion in the same units as the original data.

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N} (x_i - \mu)^2}$$

A lower standard deviation implies that the system's performance values are closely clustered around the mean, demonstrating robustness and reliability. This is particularly important for biometric authentication systems used in critical applications such as electronic voting.

Table 2 Statistical Performance Evaluation of the Proposed System

Metric	Accuracy (%)	Loss
Mean	97.8	0.46
Variance	0.0019	0.021
Standard Deviation	0.043	0.145

Table 2 summarizes the statistical evaluation of the proposed authentication model in terms of accuracy and loss values. The model achieves a high mean accuracy of **97.8%**, indicating strong overall prediction performance. The low variance value (**0.0019**) and standard deviation (**0.043**) for accuracy demonstrate that the model produces highly consistent authentication results

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

across multiple test runs. Similarly, the loss values show a relatively small mean loss (**0.46**) with moderate variance (**0.021**) and standard deviation (**0.145**), indicating stable training behavior and minimal fluctuations during model optimization. Overall, these statistical measures confirm that the proposed system maintains both high reliability and consistent performance in secure voter authentication.

Conclusion

This paper presented a secure and transparent blockchain-based electronic voting system that integrates Binance Smart Chain (BSC) with AI-driven biometric authentication to address the limitations of traditional and existing e-voting platforms. By leveraging the Proof of Staked Authority (PoSA) consensus mechanism, the proposed framework achieves fast transaction validation while maintaining decentralization and system integrity. The integration of ResNet-101–based facial recognition, combined with OTP verification and live location tracking, effectively prevents identity fraud, proxy voting, and unauthorized access. The implementation results demonstrate that the proposed system achieves high authentication accuracy, low processing latency, and strong resistance to common cyber threats, including vote tampering and impersonation attacks. The use of smart contracts ensures automated and transparent vote recording and counting, eliminating human intervention and reducing the likelihood of errors. Statistical and performance analyses further confirm the system's stability, scalability, and reliability under large-scale election scenarios. Overall, the proposed blockchain-powered e-voting framework establishes a fraud-resistant, verifiable, and trustworthy digital election model, significantly enhancing voter confidence and democratic integrity. This work highlights the potential of combining blockchain technology and deep learning to modernize electoral systems and provides a strong foundation for the development of future secure digital governance solutions.

Future Work

While the proposed blockchain-based e-voting system demonstrates strong security, transparency, and reliability, several enhancements can be explored to further improve its performance and scalability. Future work may focus on optimizing the real-time facial recognition module by employing lightweight deep learning models or edge-computing techniques to reduce computational overhead and improve response time during large-scale elections. Scalability can be further enhanced by integrating layer-2 blockchain solutions or sharding mechanisms to support national-level elections with millions of voters while maintaining low latency and minimal gas costs. Additionally, incorporating privacy-preserving techniques such as zero-knowledge proofs or homomorphic encryption could strengthen voter anonymity without compromising auditability.

The system can also be extended to support cross-chain interoperability, enabling integration with multiple blockchain platforms for improved fault tolerance and decentralization. Furthermore, future implementations may explore the use of multi-modal biometric authentication, such as combining facial recognition with fingerprint or iris recognition, to further enhance security. Finally, real-world deployment and large-scale pilot testing under diverse network conditions would provide valuable insights into system robustness, usability, and adoption. These enhancements will contribute to the evolution of a more secure, scalable, and inclusive digital voting

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

infrastructure for modern democratic governance.

References

[1]. B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE International Conference on Blockchain, pp. 1–6, 2019.

[2]. G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application," IEEE Access, vol. 9, pp. 1–12, 2021.

[3]. S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," IEEE Transactions on Network Science and Engineering, vol. 6, no. 4, pp. 1–10, 2019.

[4]. A. Alkhodre et al., "A survey on privacy-preserving blockchain systems and a novel PPBS-based framework for smart agriculture," IEEE Access, vol. 9, pp. 1–15, 2021.

[5]. 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. 10, pp. 1–12, 2021.

[6]. I. Singh, A. Kaur, P. Agarwal, and S. M. Idrees, "Enhancing security and transparency in online voting through blockchain decentralization," SN Computer Science, Springer, pp. 1–15, 2023.

[7]. B. Wang, F. Guo, Y. Liu, B. Li, and Y. Yuan, "An efficient and versatile e-voting scheme on blockchain," Cybersecurity, Springer, pp. 1–20, 2024.

[8]. U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system: Review and open research challenges," Sensors, vol. 21, no. 17, pp. 1–25, 2021.

[9]. H. O. Ohize, A. J. Onumanyi, B. U. Umar, L. A. Ajao, and R. O. Isah, "Blockchain for securing electronic voting systems: A survey of architectures, trends, and challenges," Cluster Computing, Springer, pp. 1–25, 2024.

[10]. B. Jayakumari, S. Suganya, L. Sheeb, M. Jawahar, and M. Eapen, "E-voting system using cloud-based hybrid blockchain technology," Blockchain: Research and Applications, Elsevier, pp. 1–12, 2024.

[11]. M. H. Berenjestanaki, H. R. Barzegar, and N. El Ioini, "Blockchain-based e-voting systems: A technology review," Electronics, vol. 13, no. 1, pp. 1–18, 2024.

[12]. S. El Kafhali, "Blockchain-based electronic voting system: Significance and requirements," Security and Communication Networks, Wiley, pp. 1–15, 2024.

[13]. A. Nagaria and C. Shingadiya, "Design and evaluation of a blockchain-based framework for secure and transparent digital voting systems," International Journal of Computational and Experimental Science and Engineering, pp. 1–10, 2025.

[14]. M. A. U. Khan and S. S. Tarin, "A comprehensive analysis of blockchain-based voting systems," ACM International Conference on Digital Governance, pp. 1–10, 2025.

[15]. M. J. H. Faruk, F. Alam, M. Islam, and A. Rahman, "Transforming online voting using blockchain and biometric

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1174-1182
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0166

verification," Cluster Computing, Springer, pp. 1–20, 2024.

[16]. Q. Zheng, J. Ye, P. Li, and J. Lai, "Secure and editable blockchain voting system based on chameleon hash," IET Information Security, pp. 1–12, 2024.

[17]. H. Y. Haibo, "An efficient e-voting system for business intelligence innovation based on blockchain," Journal of Intelligent & Fuzzy Systems, Springer, pp. 1–15, 2024.

[18]. H. Echchaoui and R. Boudour, "Secure and decentralized Algerian e-voting system based on blockchain and NFC," International Journal of Intelligent Systems and Applications in Engineering, pp. 1–10, 2025.

[19]. F. Rahmad and M. A. Mazlan, "Blockchain adoption in e-voting in Malaysian higher education," Environment-Behaviour Proceedings Journal, pp. 1–8, 2023.

[20]. S. H. Said, R. S. Sinde, E. M. Kosia, and M. A. Dida, "Blockchain-based system for educational qualification verification," IEEE Access, pp. 1–15, 2024.