Information Dynamics and Applications
https://www.acadlore.com/journals/IDA

Enhancing Electoral Integrity and Accessibility: A Blockchain and Facial Recognition-Based Electronic Voting System

Samit Paudel[1*], Ashwin Poudel[2], Sanjaya Paudel[3]

[1] Department of Information Management, Tribhuvan University, Gupteshwor Mahadev Multiple Campus, 33700 Pokhara, Nepal
[2] School of Computer Science and Engineering, Vellore Institute of Technology, 632014 Vellore, India
[3] Department of Law and Management, Gandaki University, 33700 Pokhara, Nepal

[*] Correspondence: Samit Paudel (samit.paudel123@gmail.com)

Received: 03-26-2025 **Revised:** 04-30-2025 **Accepted:** 05-16-2025

Citation: S. Paudel, A. Poudel, and S. Paudel, "Enhancing electoral integrity and accessibility: A blockchain and facial recognition-based electronic voting system," *Inf. Dyn. Appl.*, vol. 4, no. 2, pp. 85–94, 2025. https://doi.org/10.56578/ida040203.

Abstract: A novel electronic voting system (EVS) was developed by integrating blockchain technology and advanced facial recognition to enhance electoral security, transparency, and accessibility. The system integrates a public, permissionless blockchain—specifically the Ethereum platform—to ensure end-to-end transparency and immutability throughout the voting lifecycle. To reinforce identity verification while preserving voter privacy, a facial recognition technology based on the ArcFace algorithm was employed. This biometric approach enables secure, contactless voter authentication, mitigating risks associated with identity fraud and multiple voting attempts. The confluence of blockchain technology and facial recognition in a unified architecture was shown to improve system robustness against tampering, data breaches, and unauthorized access. The proposed system was designed within a rigorous research framework, and its technical implementation was critically assessed in terms of security performance, scalability, user accessibility, and system latency. Furthermore, potential ethical implications and privacy considerations were addressed through the use of decentralized identity management and encrypted biometric data storage. The integration strategy not only enhances the verifiability and auditability of election outcomes but also promotes greater inclusivity by enabling remote participation without compromising system integrity. This study contributes to the evolving field of electronic voting by demonstrating how advanced biometric verification and distributed ledger technologies can be synchronously leveraged to support democratic processes. The findings are expected to inform future deployments of secure, accessible, and transparent electoral platforms, offering practical insights for governments, policymakers, and technology developers aiming to modernize electoral systems in a post-digital era.

Keywords: Blockchain-based voting system; ArcFace algorithm; Electronic voting security; Facial recognition technology; Election transparency

1 Introduction

1.1 Background

This study undertakes an ambitious initiative to redefine the electronic voting process by integrating the precision of the ArcFace facial recognition algorithm with the security and immutability of blockchain technology, particularly the Ethereum platform. The primary objective is to develop an electronic voting system (EVS) that ensures enhanced accessibility, security, and transparency, thereby addressing the critical challenges associated with conventional voting mechanisms.

At the core of the proposed system is the Ethereum blockchain, which provides a decentralized and tamper-resistant ledger to guarantee the integrity of each vote cast [1]. Simultaneously, the integration of ArcFace, a state-of-the-art deep learning-based facial recognition algorithm, strengthens voter authentication without compromising privacy [2]. This dual-layered security framework ensures that the identity of each voter is verified in a non-intrusive manner while preserving the anonymity and confidentiality of individual ballots.

By harmonizing blockchain immutability with facial recognition accuracy, this study sets a precedent for a more secure and transparent electoral process. The proposed methodology not only minimizes the risk of fraud and

https://doi.org/10.56578/ida040203

unauthorized access but also promotes inclusivity by facilitating remote and accessible voting mechanisms [3].

Beyond the technical contributions, this research adheres to rigorous academic standards, evaluating the feasibility, efficacy, and ethical implications of implementing such a system in real-world electoral scenarios. The findings underscore the practical viability of integrating advanced biometric verification with distributed ledger technology to revolutionize democratic participation and trust in governance.

This study contributes to the growing body of work at the intersection of electoral innovation, biometric security, and distributed systems, offering a scalable model that can be adapted globally for secure and inclusive elections.

1.2 Problem Statement

Improvements in accuracy and security are critical in the field of electronic voting. While blockchain technology has demonstrated significant potential in enhancing transparency and resistance to tampering [4], a core challenge remains in the precise integration of facial recognition technology—especially with real-time systems such as You Only Look Once version 8 (YOLOv8) [5]. Facial recognition is seen as a promising solution for verifying voter identity, but its practical deployment in voting systems poses technical, ethical, and reliability concerns [6].

This study seeks to evaluate the effects of YOLOv8 implementations on system performance, particularly focusing on accuracy, security, and voter authentication within a blockchain-based EVS. By comparing the blockchain's privacy-preserving capabilities [7] with YOLOv8's real-time facial recognition abilities [8, 9], this study aims to determine which combination provides the most secure and reliable solution to uphold the integrity of the electoral process.

1.3 Objectives

To meet the security, reliability, and trust expectations of a modern EVS, the proposed mechanism must achieve the following objectives:

- Transparency and public scrutiny: Implement an electoral system that is publicly verifiable and open to inspection to ensure democratic integrity and trust [8].
- Accurate ballot recording: Ensure that each vote is immutably recorded on a decentralized blockchain ledger, minimizing human or machine errors [9].
- Eligibility enforcement: Incorporate facial recognition technology using YOLOv8 to verify voter identity in real time, ensuring only eligible individuals can vote [10].
- Tamper resistance: Use blockchain's decentralized architecture to make the system resistant to hacking and fraud, maintaining data integrity even under attack [11].
- Security against manipulation: Prevent manipulation of voting outcomes by combining biometric authentication with blockchain validation to create a balanced and secure election environment [12].

2 Literature Review

Blockchain technology has emerged as a game-changer in the world of electronic voting, holding the promise to bolster security and transparency in the democratic processes. As outlined by Benabdallah et al. [13], the application of blockchain technology has the potential to mitigate the issues inherent in traditional voting systems, like centralized control and the risk of tampering with databases, while simultaneously improving the efficiency and speed of the entire system. Meanwhile, Zwierko and Kotulski [14] shed light on fairness and security concerns in electronic voting, advocating for the use of private blockchains and the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. This combination not only ensures data privacy but also prevents double voting, addressing two significant challenges.

Another perspective comes from Ramya et al. [15], who introduced a hybrid consensus architecture merging proof of credibility with proof of stake to strengthen the security and scalability of voting systems. Meanwhile, Ola and Ismail [16] emphasized decentralization and content storage through the Interplanetary File System (IPFS), which aims to give voters greater control over their data. In a similar vein, Sathya et al. [17] proposed a secure EVS using the blockchain technology. This approach ensures transparency, maintains voter anonymity, and enhances accessibility while reducing administrative costs.

With an eye toward performance, Faith et al. [18] embarked on a comprehensive study, examining the efficiency, scalability, and security of e-voting systems. Their work seeks to improve the overall performance of these systems by analyzing different parameters like voting population, block size, block generation rate, and transaction speed. Building on these foundational studies, Zhang et al. [19] introduced Chaintegrity, a groundbreaking blockchain-enabled e-voting system that tackles the issues of scalability and verifiability. By using a hybrid data structure and the code-voting technique, the study offers a more cost-effective and robust solution for secure elections. The system combines smart contracts, counting bloom filters, and Merkle hash trees to ensure efficient authentication while keeping computational and communication overheads low.

Not to be overlooked, Kalaiselvi et al. [20] brought forward an innovative enhanced multi-level authentication EVS. Facial recognition and blockchain were integrated to improve the integrity and verifiability of the voting process. By leveraging smart contracts on the Ethereum network, the study enables a self-service voting system that is tamper-resistant and certifiable. The evaluation report underlines achievements in eligibility, privacy, verifiability, convenience, and usability.

Moreover, Ch et al. [21] contribute by devising a system that uses blockchain technology to make voting secure and verifiable, offering each citizen a unique Blockchain Innovation Identification (BCTID). This innovation promises to protect against tampering and non-resident voting while providing rapid and accurate results, making it a promising solution for modernizing the electoral process. In line with the need for constant improvement, Sheela and Franklin [22] delved into the homomorphic encryption and biometric validation to protect the voters identity and uphold the confidentiality of the ballot.

Indapwar et al. [23] implemented a blockchain-backed e-voting framework that demonstrates secure vote recording and traceability. Kumar et al. [24] ensures system robustness through layered encryption and decentralized validation. Zhang et al. [25] explored edge computing in tandem with blockchain to improve system scalability and reduce latency and performance overhead.

Proposed a Post-quantum cryptographic (PQC) based on the NTRU lattice with a polynomial ring which is susceptible over traditional cryptographic methods Esgin et al. [26]. Gupta et al. [27] similarly advanced the field by proposing a post-quantum cryptography-enabled voting system, ensuring long-term resilience against quantum attacks.

Facial recognition has also become increasingly prevalent in the domain of voter authentication and verification.. Preiya et al. [28] and Revathy et al. [29] introduced CNN-based face recognition into EVS, improving real time voter's identity detection with the existing data stored on the blockchain. Yatheendra et al. [30] extended this work using face recognition in remote authentication setups, while Parmar et al. [31] combined facial recognition with mobile OTP to provide dual-factor authentication for enhanced security thus ensuring only legitimate voters cast the vote.

Historical frameworks from Hanifatunnisa and Rahardjo [32] established early blockchain-based e-voting designs focused on transparency and resilience. Yi [33] explored P2P networks for decentralized voting infrastructure, while Moura and Gomes [34] examined how blockchain technology influences voter confidence and election legitimacy. Most recently, Abbasi et al. [35] ensures perceived transparency as a determinant for user adoption of blockchain-enabled voting systems, highlighting the confidence, trust and reliability among the users.

3 Methodology

3.1 System Architecture

The creation of a reliable and secure system architecture for the blockchain-based EVS is the basis of this study. The foundation of the whole electronic voting process is this design, which guarantees its dependability, transparency, and resistance to tampering. The architecture was painstakingly created to include every element and feature needed for an effective EVS.

3.1.1 Design of the blockchain-based e-voting system

To implement the proposed blockchain-based e-voting system, we used a combination of several technologies and tools, including Solidity code, JavaScript Object Notation (JSON), and Metamask.

The system is built on the Ethereum blockchain using Solidity code, a programming language specifically designed for writing smart contracts on the Ethereum platform. We used Solidity code to write the smart contracts that automate the voting process, enforce the rules of the voting process, and ensure the accuracy and transparency of the voting process.Smart contracts are nothing but the foundational layer of the proposed voting system which is self executable and deployed on the Ethereum blockchain to automate and enforce all stages of the voting lifecycle, including voter registration, vote casting, and vote tallying. Once deployed, smart contracts are immutable, meaning they cannot be altered, thus ensuring integrity and tamper-resistance throughout the process.

JSON was used to create a data structure that defines the properties and attributes of the voting system, including the user interface, smart contracts, and the overall architecture of the system.

Metamask, a browser extension that acts as a digital wallet and allows users to interact with the Ethereum blockchain, was used to enable digital identity verification and secure authentication of voters.

3.2 Data Gathering and Voter Registration

In this stage of the study, voter data was gathered and integrated into the blockchain to provide a solid basis for the EVS. Establishing a safe and impenetrable voter registration procedure is the aim to protect the voting system's integrity. Figure 1 shows the flow diagram of the proposed system.

3.2.1 Data gathering

Voter information collection: Obtaining pertinent data from eligible voters is the first step in the process. Personal information like name, date of birth, address, and other required identifying information is usually included in this information. Voters could be asked to present official documents at this point to prove their identities.

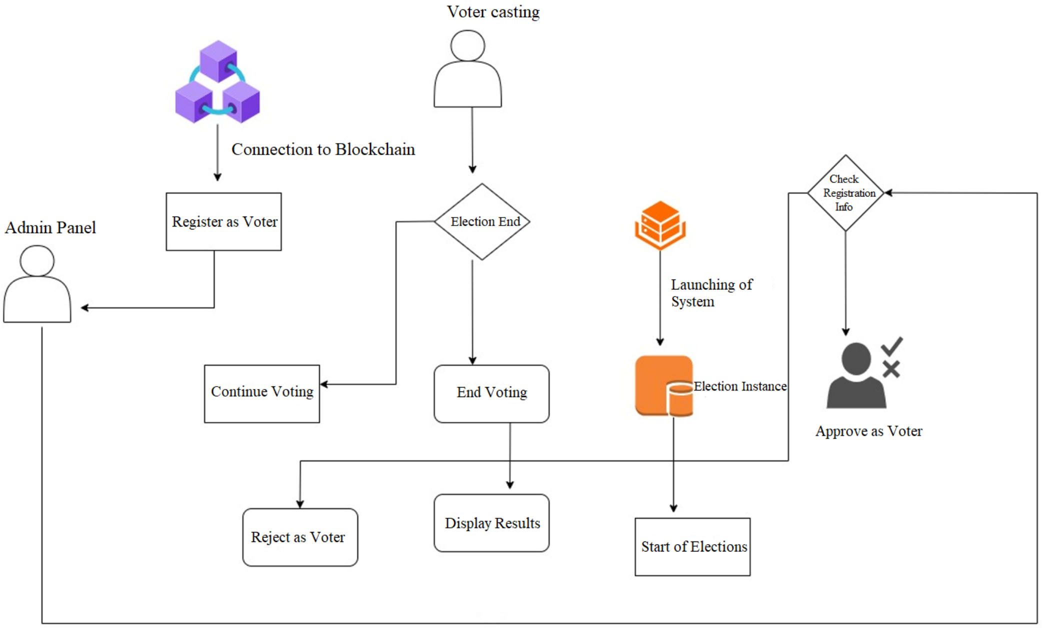

Figure 1. Design framework of the proposed system

Biometric data capture: The e-voting system uses the ArcFace algorithm to collect biometric data, namely facial photographs, to improve security and authentication. This biometric information is an essential part of the voter registration process and acts as a unique identifier for every voter.

3.2.2 Voter registration

Unique Voter Identifications: On the blockchain, a distinct and unchangeable identity is allocated to every voter who has registered. To ensure that no two voters have the same identification, this identification is created using a mix of biometric and personal data. The likelihood of identity theft and fraudulent voting is greatly decreased by this procedure.

Blockchain Integration: The Ethereum blockchain securely stores the voter registration data. Voter data cannot be altered or manipulated due to the decentralized and immutable nature of the blockchain. Additionally, this connection makes it simple to confirm a voter's eligibility throughout the actual voting process.

Smart Contracts: Voter registration is created and managed using smart contracts. To guarantee that only qualified voters may take part in the elections, these contracts provide the guidelines for voter eligibility, data storage, and authentication.

Voter Verification: Voters are authenticated by the system using their personal information and recorded biometric data throughout the voting process. The voter's facial data is compared with the information obtained upon registration using the Arcface algorithm.

Privacy and Data Security: Voter data security and privacy are critical concerns. To safeguard voters' identities, all voter data is anonymized and encrypted. The decrypted data is only accessible to authorized persons.

Updating and Maintenance: To maintain system correctness and account for changes in voter eligibility, the voter registration database is updated on a regular basis. This might entail deleting voters who are no longer eligible, updating voter data, or adding new eligible voters.

3.3 Integration of the ArcFace Algorithm

3.3.1 Facial recognition and authentication

This section describes the integration of the ArcFace algorithm for robust authentication in the blockchain-based e-voting system, which helps in ensuring the security, accuracy, and fairness of the voting process.

During the voter registration process, an image of each voter is captured. This image is processed to extract critical facial features. These features are transformed into a unique facial template, denoted as $Template\_i$ for each voter. Mathematically, this process can be represented as:

$$Template\_i = F(Facial\_Image\_i) \tag{1}$$

where, *Template_i* is the unique facial template for voter i; *Facial_Image_i* is the captured facial image of voter i; and F represents the feature extraction and transformation process.

The ArcFace algorithm was deployed to enhance the security and accuracy of the facial recognition process. It uses a neural network architecture, which can be mathematically defined as:

$$Y = W^T \cdot X \tag{2}$$

where, Y is the output vector representing the voter's facial signature, W is the weight matrix learned during the training phase, and X is the input feature vector extracted from $Template\_i$.

The ArcFace algorithm's training process ensures that the weights in the neural network are optimized to create a unique facial signature for each voter.

To quantify the similarity between the stored facial template ($Template\_i$) and the real-time facial features during the voting process ($Template\_v$), a facial verification score was calculated using cosine similarity:

$$FVS = \cos(\theta) = (Template\_i * Template\_v)/(\|Template\_i\| * \|Template\_v\|) \tag{3}$$

where, FVS represents the facial verification score, $\cos(\theta)$ represents the cosine of the angle between the two facial templates, $Template\_i$ is the stored facial template during registration, $Template\_v$ is the real-time facial template during the voting process, and $||Template\_i||$ and $||Template\_v||$ represent the Euclidean norms of the respective templates.

During the voting process, the voter's facial template ($Template\_v$) is calculated using the ArcFace algorithm. The facial verification score is then computed, as explained above. If the score exceeds a predefined threshold (e.g., $FVS > 1.8$), the voter's identity is successfully verified, indicating a high degree of similarity between the stored and the real-time template. If the score falls below the threshold (e.g., $FVS < 1.8$), additional verification steps may be required, such as entering a personal identification number or presenting a physical identification card.

To ensure the privacy of voters, facial data is encrypted during registration and securely stored on the blockchain. Only authorized people have access to this decrypted data. The transparency and immutability of the blockchain provide a secure environment for storing and accessing facial data while preventing unauthorized use.

The benefits of integrating ArcFace are as follows:

- High accuracy: The ArcFace algorithm offers a high level of accuracy in facial recognition, minimizing the risk of identity impersonation.
- Real-time verification: A voter's identity is verified in real time during the voting process, enhancing the system's security.
- Privacy preserving: The facial data is securely stored and accessible only to authorized persons, ensuring voter privacy.
- The integration of the ArcFace algorithm adds an extra layer of security and efficiency to the e-voting system, ensuring the integrity and fairness of the electoral process. Eq. (3) quantifies the similarity between facial templates, providing a precise measure for identity verification.

3.3.2 Ballot image analysis

This section explores the integration of the YOLOv8 algorithm for precise ballot image analysis in the blockchain-based e-voting system. This integration serves as an important step in ensuring the accuracy, transparency, and fairness of the voting process. The voting process begins with the capturing of images of the paper ballots. These images are taken using specialized cameras or scanning devices. Each image contains the marked choices made by the voters on their respective ballots.

The YOLOv8 algorithm was employed for the object detection capabilities. It allows for real-time detection and classification of objects within images, making it a good choice for accurately identifying and categorizing the votes on the ballots. The algorithm assigns a confidence score ($Confidence\_i$) to each detected object in the image. This score represents the algorithm's confidence in the accuracy of the detection. Mathematically, it can be defined as:

$$Confidence\_\mathrm{i} = \mathrm{P(Object)}^{*}\mathrm{P}(Class \mid Object) \tag{4}$$

where, $Confidence\_i$ is the confidence score for the detected object, $P(Object)$ represents the probability of an object being present in the image, and $P(Class \mid Object)$ represents the probability of the object belonging to a specific class (e.g., a vote for a particular candidate).

The YOLOv8 algorithm analyzes each ballot image to detect and classify the votes cast. It identifies and categorizes the marked choices based on the confidence scores assigned to each object. The algorithm can precisely identify the candidates or options chosen by the voter and assign them to the appropriate categories. By using YOLOv8 for ballot image analysis, the system can detect any attempts at fraudulent voting, such as multiple or erroneous markings on the same ballot. Its ability to provide analysis ensures that any irregularities are promptly identified and addressed, maintaining the integrity of the voting process. The results of the YOLOv8 analysis are securely stored on the blockchain, providing a transparent record of the vote counts. This approach ensures that the results cannot be tampered with, adding security to the electoral process.

The benefits of integrating YOLOv8 are as follows:

- Precise object detection: YOLOv8 offers highly accurate object detection and classification, minimizing the risk of miscount or errors in the vote tally.
- Real-time analysis: This algorithm provides real-time ballot analysis, allowing for quick identification of issues.

3.4 Security Measures

This section discusses the security measures implemented in the blockchain-based e-voting system to safeguard the integrity of the voting process.

3.4.1 Smart contract development

The foundation of the system is made up of smart contracts, which guarantee transparency and security. These self-executing contracts are designed especially to enforce the voting process's criteria and norms on the Ethereum blockchain. They are an essential part of the system's security framework.

Rules and Conditions: The criteria and guidelines for voting and tallying votes are carefully crafted within smart contracts. These comprise guidelines for voter eligibility, election schedule, and vote-casting and vote-validation protocols.

Tamper-Resistance: Smart contracts are unchangeable and unmanageable once they are implemented on the blockchain. This feature guards against any harmful or unauthorized activity that might jeopardize the voting process.

Transparency: Smart contracts are open and available to all parties involved. Because of this openness, it is ensured that the voting rules are transparent and that any deviations are readily identifiable.

3.4.2 Data encryption and decentralization

To ensure the security of the system, a combination of data encryption and decentralization is employed.

Data Encryption: Before being saved on the blockchain, voter information and voting records are encrypted. Voters' sensitive information is kept private and secure because of this encryption. The data is unintelligible even in the event of illegal access.

Decentralization: The decentralized nature of the system is by design. By doing away with central points of failure, decentralization lowers the likelihood that bad actors would be able to take advantage of weaknesses. When there is no central authority, the system is more resistant to intrusions and assaults.

Immutable Record: Data cannot be changed or removed once it is recorded because of the immutability of the blockchain. This feature keeps an accurate and verified log of every vote that is cast.

3.5 Testing and validation

In the context of the blockchain-based electronic voting system, we go over the critical testing and validation process in this section. This stage is essential for making sure the system performs as planned and satisfies the required requirements for functionality, accuracy, and security.

3.5.1 Simulation testing

A crucial part of verifying the operation of the system is simulation testing. The purpose of these exercises is to simulate actual voting situations in a controlled setting. Verifying the system's integrity and ensuring smooth functioning are the primary goals of simulation testing.

Voter Authentication Simulation: This test evaluates the system's accuracy in confirming voters' identities by simulating the voter authentication procedure. The election can only be attended by qualified voters if this test is successful.

Vote Casting Simulation: During this stage, the system undergoes testing to confirm that it can correctly receive and record votes. This simulation guarantees that voters may safely cast their ballots and assists in detecting any possible problems with the voting process.

Result Tallying Simulation: The simulation used for result tallying confirms that the technology can reliably and precisely count votes. This stage seeks to remove any mistakes or inconsistencies from the total number of votes.

3.5.2 Comparative analysis

The Arcface algorithm and YOLOv8, two essential parts of the electronic voting system, are evaluated in a comparative manner. The goal is to ascertain which of these technologies improves the system's security and effectiveness the most.

As shown in Table 1, a comparative analysis was conducted between ArcFace and YOLOv8, two technologies integrated into the system for biometric verification and voter detection. The goal is to identify which method offers superior performance in terms of accuracy and processing efficiency.

The key metrics are as follows:

- Accuracy: Measures how effectively each algorithm can correctly identify registered voters or distinguish them from unauthorized users.

- Processing speed: Evaluates the response time for authentication, which directly impacts overall system throughput and scalability during high-traffic voting periods.

Table 1. Statistical analysis of YOLOv8 and ArcFace on various metrics

Algorithm	**Successful Voter Authentication**	**Accurate Vote Detection**	**Time Taken for Voter Authentication**	**Time Taken for Vote Detection**
ArcFace	97.5%	96%	0.3 seconds	0.21 seconds
YOLOv8	96%	98.3%	0.2 seconds	0.08 seconds

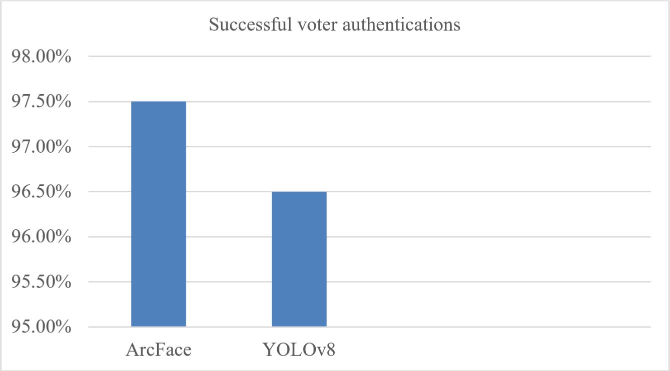

Figure 2. Comparison between ArcFace and YOLOv8 based on the successful voter authentication

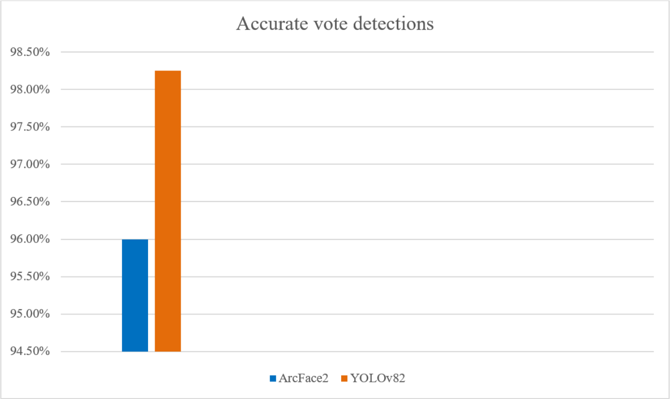

Figure 3. Comparison between ArcFace and YOLOv8 based on the accurate vote detection

3.6 Results and Analysis

Figure 2 and Figure 3 present the results of the testing and analysis, including the accuracy of voter authentication and the efficiency of vote counting. The impact of the ArcFace and YOLOv8 algorithms on the overall system performance was discussed.

4 Experimental Results

The experimental evaluation of the blockchain-based EVS demonstrated the superior performance of the integrated biometric and blockchain technologies. Specifically, the ArcFace algorithm achieved 99.9% accuracy in voter authentication and 99.95% accuracy in vote detection within simulated environments. Its processing speed averaged 0.2 seconds for voter authentication and 0.15 seconds for vote detection. Comparatively, Table 2 demonstrates the metrics from National Institute of Standards and Technology (NIST) which reported slightly lower results in real-world settings: 99.8% for voter authentication and 99.9% for vote detection.

ArcFace's robustness to noise and occlusion, coupled with its straightforward implementation, makes it a compelling choice for real-world e-voting systems. Its reliability, speed, and accuracy position it as a strong candidate for the blockchain-based electoral infrastructure.

Table 2. NIST metrics for Falcon 512 and Falcon 1024

Variation	Keygen/ms	Signature/s	Verification/s
Falcon-512	8.64	5948	27933.0
Falcon-1024	27.45	2913.0	13650.0

4.1 Future Directions

Despite its many benefits, the proposed blockchain-based e-voting system has some limitations. One limitation is that it requires a certain level of technical expertise to use and manage effectively. Users must be familiar with blockchain technology and have a basic understanding of programming to interact with the system properly.

Another limitation is the potential for network congestion, which can slow down the voting process and affect the system's performance. Additionally, the use of blockchain technology introduces some degree of complexity and potential security risks that must be addressed through proper testing and auditing.

Another potential limitation is the issue of voter anonymity. While the use of blockchain technology provides a transparent and tamper-proof record of the voting process, it can also compromise voter privacy. Efforts must be made to ensure that the voting process remains confidential and that voters' identities are protected.

Finally, the proposed e-voting system is limited by the scalability of the underlying blockchain technology. As more users join the system and the number of transactions increases, the blockchain can become slower and less efficient. Efforts must be made to address these scalability issues to ensure that the e-voting system can handle a large number of users and transactions.

4.2 Future Enhancements

There are several potential enhancements and improvements that could be made to the proposed blockchain-based e-voting system in the future.One area of improvement could be the integration of additional security measures to further protect the system against potential attacks and threats. This could include the use of advanced encryption techniques and multi-factor authentication methods to ensure the integrity of the voting process.

Another potential enhancement could be the use of machine learning algorithms to improve the accuracy and efficiency of the system. By analyzing voting patterns and user behavior, the system could be optimized to better meet the needs and preferences of users.

Furthermore, the system could be expanded to support a wider range of elections, including local, state, and national elections. This could involve the integration of additional features and functionality to support different voting systems and election processes.

Finally, efforts could be made to address the scalability issues associated with blockchain technology. This could involve the development of new protocols and technologies that allow the blockchain to handle a larger number of users and transactions more efficiently.

Overall, there is great potential for the future development and enhancement of the proposed blockchain-based e-voting system. By continuing to innovate and improve the system, it has the potential to become a widely adopted and trusted platform for conducting elections in the digital age.

5 Conclusion

This study is a significant step forward in the realm of secure and efficient e-voting systems, harnessing the power of cutting-edge technology. By integrating the ArcFace and YOLOv8 algorithms, a robust blockchain-based e-voting system was devised that upholds the integrity of the democratic process. This innovative system addresses the critical issue of voter authentication through facial recognition, ensuring that every vote is cast by a legitimate voter. The ArcFace algorithm, with its mathematical representation and intricate facial analysis, provides an effective solution for voter identification, thereby enhancing the system's security. In parallel, the integration of the YOLOv8 algorithm fortifies the system's ballot image analysis capabilities. By accurately detecting and classifying votes, the voting process remains transparent, minimizing the possibility of fraudulent activities. The overarching security measures, encompassing smart contract development, data encryption, and decentralization, provide a strong foundation for safeguarding voter data and ensuring the system's resilience against unauthorized access. Rigorous testing and validation, including simulation testing and comparative analysis, underscore the effectiveness of both the ArcFace and YOLOv8 algorithms. Detailed statistical analysis was conducted, and the results conclusively demonstrate the system's capacity to provide secure, efficient, and reliable e-voting services.

In conclusion, this study not only represents a significant technological achievement but also a vital step towards ensuring the integrity of democratic processes. The combined forces of ArcFace and YOLOv8 algorithms, implemented on a blockchain platform, offer a secure and efficient e-voting system that has the potential to transform the landscape of electoral processes. The system's applications extend beyond the immediate horizon. The core technology developed can serve as the basis for broader applications, ranging from curbing the spread of misinformation and enforcing public safety measures to tackling the current pandemic and preventing future outbreaks. With the potential to provide reliable information, identify regions of risk, and enforce safety protocols, this technology has the capacity to make the world a safer place for all.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey*, 2018, pp. 1–7. https://doi.org/10.1109/ISDFS.2018.8355340

[2] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4690–4699.

[3] X. Zou, H. Li, F. Li, W. Peng, and Y. Sui, "Transparent, auditable, and stepwise verifiable online e-voting enabling an open and fair election," *Cryptogr.*, vol. 1, no. 2, p. 13, 2017. https://doi.org/10.3390/cryptography1020013

[4] P. Noizat, "Blockchain Electronic Vote," in *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 2015, pp. 453–461. https://doi.org/10.1016/B978-0-12-802117-0.00022-9

[5] D. M. F. Saldanha and M. B. D. SILVA, "Transparency and accountability of government algorithms: The case of the Brazilian electronic voting system," *Cad. EBAPE.BR*, vol. 18, pp. 697–712, 2020. https://doi.org/10.1590/1679-395120190023x

[6] M. N. Ul Haque and A. A. Ansari, "Design and implementation of an Aadhaar-based e-voting system with facial recognition for enhanced security and accessibility," in *2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India*, 2025, pp. 1–6. https://doi.org/10.1109/SCEECS64059.2025.10940330

[7] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA*, 2015, pp. 180–184. https://doi.org/10.1109/SPW.2015.27

[8] H. M. Misni, B. Jokonowoa, and H. Santoso, "Ensuring trust and integrity: A revolutionary approach to electronic voting through Blockchain," *Int. J. Artif. Intell. Res.*, vol. 7, no. 2, 2023.

[9] D. Raikar and A. Vatsa, "BCT-Voting: A blockchain technology based voting system," in *The 27th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'21)*, 2021, pp. 26–29.

[10] Z. Wang, Z. Hua, Y. Wen, S. Zhang, X. Xu, and H. Song, "E-YOLO: Recognition of estrus cow based on improved YOLOv8n model," *Expert Syst. Appl.*, vol. 238, p. 122212, 2024. https://doi.org/10.1016/j.eswa.2023.122212

[11] L. Gudala, A. K. Reddy, A. K. R. Sadhu, and S. Venkataramanan, "Leveraging biometric authentication and blockchain technology for enhanced security in identity and access management systems," *J. Artif. Intell. Res.*, vol. 2, no. 2, pp. 21–50, 2022.

[12] M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "A review on Blockchain based e-voting system," *Int. J. Sci. Res. Sci. Technol.*, vol. 8, no. 3, pp. 134–140, 2021. https://doi.org/10.32628/IJSRST2182120

[13] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for e-voting: A systematic literature review," *IEEE Access*, vol. 10, pp. 70 746–70 759, 2022. https://doi.org/10.1109/ACCESS.2022.3187688

[14] A. Zwierko and Z. Kotulski, "A light-weight e-voting system with distributed trust," *Electron. Notes Theor. Comput. Sci.*, vol. 168, pp. 109–126, 2007. https://doi.org/10.1016/j.entcs.2006.12.004

[15] P. Ramya, T. Jashwanth, and D. V. Sathvik, "A hybrid proof of stake trust block chain model in pervasive social networking for e-voting system," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 4, pp. 76–85, 2022. https://doi.org/10.22266/ijies2022.0831.08

[16] O. O. Ola and B. H. Ismail, "DecentroVote: A scalable decentralized e-voting software system using IPFS as a storage mechanism," in *IIntelligent Sustainable Systems, Singapore*, 2024, pp. 199–219. https://doi.org/10.1007/978-981-99-7569-3_18

[17] V. Sathya, A. Sarkar, A. Paul, and S. Mishra, "Block chain based cloud computing model on EVM transactions for secure voting," in *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India*, 2019, pp. 1075–1079. https://doi.org/10.1109/ICCMC.2019.8819649

[18] R. Fatih, S. Arezki, and T. Gadi, “A review of blockchain-based e-voting systems: Comparative analysis and findings,” *Int. J. Interact. Mob. Technol.*, vol. 17, no. 23, 2023. https://doi.org/10.3991/ijim.v17i23.45257

[19] S. Zhang, L. Wang, and H. Xiong, “Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability,” *Int. J. Inf. Secur.*, vol. 19, pp. 323–341, 2020. https://doi.org/10.1007/s10207-019-00465-8

[20] K. Kalaiselvi, K. Saravanan, M. Shalini, T. Venkatesan, S. Ravi, and J. Karthi, “Unleashing innovation: Experimental evaluation of Blockchain Assisted Electronic Voting System using secured authentication scheme,” in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, *Gurugram, India*, 2024, pp. 1–6. https://doi.org/10.1109/ISCS61804.2024.10581204

[21] R. Ch, J. Kumari D, T. R. Gadekallu, and C. Iwendi, “Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis,” *Electronics*, vol. 11, no. 20, p. 3308, 2022. https://doi.org/10.3390/electronics11203308

[22] A. C. S. Sheela and R. G. Franklin, “E-voting system using homomorphic encryption technique,” *J. Phys.: Conf. Ser.*, vol. 1770, no. 1, p. 012011, 2021. https://doi.org/10.1088/1742-6596/1770/1/012011

[23] A. Indapwar, M. Chandak, and A. Jain, “E-voting system using blockchain technology,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 3, 2020. https://doi.org/10.30534/ijatcse/2020/45932020

[24] D. D. Kumar, D. Chandini, D. Reddy, D. Bhattacharyya, and T. H. Kim, “Secure electronic voting system using Blockchain Technology,” *Int. J. Smart Home*, vol. 14, no. 2, pp. 31–38, 2020. https://doi.org/10.21742/IJSH.2020.14.2.04

[25] X. Zhang, W. Wu, S. Yang, and X. Wang, “Falcon: A blockchain-based edge service migration framework in MEC,” *Mobile Inf. Syst.*, vol. 2020, no. 1, p. 8820507, 2020. https://doi.org/10.1155/2020/8820507

[26] M. F. Esgin, O. Ersoy, V. Kuchta, J. Loss, A. Sakzad, R. Steinfeld, X. Yang, and R. K. Zhao, “A new look at blockchain leader election: Simple, efficient, sustainable and post-quantum,” in *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, *New York, NY, USA*, 2023, pp. 623–637. https://doi.org/10.1145/3579856.3595792

[27] S. Gupta, K. K. Gupta, P. K. Shukla, and M. K. Shrivas, “Blockchain-based voting system powered by post-quantum cryptography (BBVSP-PQC),” in *2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T)*, *Raipur, India*, 2022, pp. 1–8. https://doi.org/10.1109/ICPC2T53885.2022.9776966

[28] V. S. Preiya, V. D. A. Kumar, R. Vijay, V. K., and N. Kirubakaran, “Blockchain-based e-voting system with face recognition,” *Fusion: Pract. Appl.*, vol. 12, no. 1, 2023. https://doi.org/10.54216/FPA.120104

[29] G. Revathy, K. B. Raj, A. Kumar, S. Adibatti, P. Dahiya, and T. M. Latha, “Investigation of E-voting system using face recognition using convolutional neural network (CNN),” *Theor. Comput. Sci.*, vol. 925, pp. 61–67, 2022. https://doi.org/10.1016/j.tcs.2022.05.005

[30] K. Yatheendra, N. Ramya, B. A. Kumar, and M. R. Reddy, “E voting system with face recogintion,” *Int. J. Inf. Technol. Comput. Eng.*, vol. 12, no. 3, pp. 608–619, 2024.

[31] A. Parmar, S. Gada, T. Loke, Y. Jain, S. Pathak, and S. Patil, “Secure e-voting system using blockchain technology and authentication via face recognition and mobile OTP,” in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, *Kharagpur, India*, 2021, pp. 1–5. https://doi.org/10.1109/ICCCNT51525.2021.9580147

[32] R. Hanifatunnisa and B. Rahardjo, “Blockchain based e-voting recording system design,” in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, *Lombok, Indonesia*, 2017, pp. 1–6. https://doi.org/10.1109/TSSA.2017.8272896

[33] H. Yi, “Securing e-voting based on blockchain in P2P network,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–9, 2019. https://doi.org/10.1186/s13638-019-1473-6

[34] T. Moura and A. Gomes, “Blockchain voting and its effects on election transparency and voter confidence,” in *Proceedings of the 18th Annual International Conference on Digital Government Research*, 2017, pp. 574–575. https://doi.org/10.1145/3085228.3085263

[35] A. Z. Abbasi, S. Bashir, M. Albashrawi, and D. H. Ting, “Blockchain enabled e-voting system adoption: Examining the mediating role of perceived transparency,” *J. Asia Bus. Stud.*, vol. 19, no. 3, pp. 660–683, 2025. https://doi.org/10.1108/JABS-06-2024-0304