International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 05 | May 2026 www.irjet.net p-ISSN: 2395-0072

De-Centralized E-Voting System with Face-recognition

Mr. Suraj Pawar[1], Vishwajeet Mahadik[2], Shrikant Pilave[3], Vaibhav Kumbhar[4], Prof. shrikant Kadam[5]

[1] *B.Tech Student, Dept of Computer Engineering, JCEP College KM Gad Sangli, Maharashtra, India*

[2] *B.Tech Student, Dept of Computer Engineering, JCEP College KM Gad Sangli, Maharashtra, India*

[3] *B.Tech Student, Dept of Computer Engineering, JCEP College KM Gad Sangli, Maharashtra, India*

[4] *B.Tech Student, Dept of Computer Engineering, JCEP College KM Gad Sangli, Maharashtra, India*

[5] *Associate Professor, Dept of Computer Engineering, JCEP College KM Gad Sangli, Maharashtra, India*

Abstract - *Electronic voting systems are becoming increasingly important due to the growing demand for secure, transparent, and efficient election processes. Traditional voting methods often face challenges such as centralized control, vote tampering, voter impersonation, lack of transparency, and slow vote counting. This paper presents a Decentralized E-Voting System using Blockchain and Face Recognition to overcome these limitations by combining blockchain technology with biometric authentication. The proposed system uses Ethereum blockchain and Solidity smart contracts to ensure secure, transparent, and tamper-proof vote recording. A hybrid storage model is implemented in which important voting data is stored on-chain, while large files such as identity documents and facial images are maintained off-chain to improve storage efficiency. Face recognition authentication is implemented using OpenCV and the LBPH algorithm to verify voter identity and prevent unauthorized voting. The backend of the system is developed using FastAPI, while HTML, CSS, and JavaScript are used to build the frontend interface. The system supports administrator, voter, and candidate roles for secure election management and real-time result generation. Experimental results show that the proposed system improves election security, transparency, and reliability while reducing manual intervention and the risk of double voting.*

***Key Words*: Blockchain, Electronic Voting, Decentralized Voting System, Ethereum, Smart Contracts, Face Recognition, Transparency, FastAPI, OpenCV**

1. INTRODUCTION

The rapid growth of digital technology has transformed many sectors such as banking, healthcare, education, and governance. Despite these advancements, voting systems in several regions still depend on traditional methods that are often slow, inefficient, and vulnerable to fraud or manipulation. Maintaining transparency, security, and public trust during elections continues to be a major challenge in modern democratic systems. Even existing electronic voting systems face issues because of centralized architectures, which increase the risk of data tampering, unauthorized access, and system failure.

Blockchain technology has emerged as a reliable solution for developing secure and decentralized applications. Features such as decentralization, immutability, transparency, and cryptographic security make blockchain highly suitable for electronic voting systems. By recording votes on a distributed ledger, blockchain helps ensure that election data cannot be modified once stored and allows transparent verification of results without relying on a central authority.

This research presents a Decentralized E-Voting System using Blockchain and Face Recognition to provide a secure and transparent digital voting platform. The proposed system integrates Ethereum blockchain technology with biometric authentication to strengthen voter verification and election integrity. Smart contracts developed using Solidity automate important election operations such as

voter registration, candidate verification, election management, vote casting, and result generation.

To improve authentication security, the system uses face recognition technology implemented with OpenCV and the Local Binary Pattern Histogram (LBPH) algorithm. During registration, voters upload facial data that is later used for identity verification during voting. This process reduces the chances of impersonation and unauthorized voting.

The proposed system follows a hybrid architecture in which critical election data and voting transactions are stored on the blockchain, while large files such as facial images and identity documents are maintained off-chain. This approach improves scalability, reduces blockchain storage costs, and maintains data integrity through cryptographic hashing techniques. The backend is developed using FastAPI and Web3.py for blockchain interaction, while HTML, CSS, and JavaScript are used to create a user-friendly frontend interface. The system supports different user roles including administrator, voter, and candidate for efficient election management and secure participation.
The proposed decentralized voting platform aims to overcome the limitations of traditional voting systems by improving transparency, preventing double voting, strengthening voter authentication, and reducing manual intervention. The project demonstrates how blockchain and biometric technologies can be combined to develop secure and reliable next-generation electronic voting systems for educational institutions, organizations, and future large-scale applications.

2. LITERATURE REVIEW

The rapid growth of digital technologies and increasing concerns regarding election security have encouraged researchers to explore blockchain technology as a reliable solution for modern electronic voting systems. Traditional voting methods often face problems such as centralized control, vote tampering, lack of transparency, voter impersonation, and delays in result generation. To overcome these challenges, many researchers have focused on developing decentralized voting frameworks using blockchain technology, smart contracts, and biometric authentication techniques.
M. M. H. Onik et al. [1] discussed the importance of blockchain technology in Industry 4.0 applications and explained its potential in secure electronic voting systems. Their study highlighted important blockchain features such as decentralization, transparency, immutability, and secure transaction management, which make blockchain suitable for modern digital elections. However, the authors also pointed out challenges related to scalability, privacy, and implementation complexity in blockchain-based voting systems.

A. K. Singh and R. Kumar [2] reviewed blockchain-based electronic voting systems and concluded that blockchain technology improves election transparency and reduces the risk of vote manipulation. Their research mainly focused on distributed ledger architecture and secure vote recording mechanisms. Similarly, S. Pawar and R. Sharma [3] proposed a smart contract-based e-voting framework using Ethereum blockchain. Their work demonstrated that Solidity smart contracts can automate voting operations and reduce manual intervention in election management.

H. Patel and D. Shah [4] developed a decentralized voting system using Ethereum blockchain and explained how distributed ledger technology helps prevent unauthorized modifications to voting records. Their study also emphasized the importance of cryptographic security and transparency in decentralized election systems. P. Sharma and A. Verma [5] further extended this concept by integrating biometric authentication with blockchain voting systems. Their research showed that combining blockchain technology with biometric verification improves voter authentication and reduces impersonation attacks.

M. Gupta and S. Jain [6] implemented a smart contract-based e-voting system and demonstrated that Ethereum smart contracts can efficiently automate voter registration, vote casting, and result generation processes. K. Rathi and V. Kulkarni [7] proposed a blockchain-powered transparent voting mechanism that focused on improving public trust through immutable and transparent vote storage. Similarly, T. Nguyen and L. Tran [8] introduced a secure e-voting framework using Ethereum blockchain and analyzed how decentralized architecture improves election integrity and prevents data tampering.

Authentication and voter verification have become important research areas in modern voting systems. R. Mehta and P. Deshmukh [9] proposed a face recognition-based authentication mechanism for secure electronic voting. Their work demonstrated that biometric verification can reduce voter impersonation and improve election security. Likewise, R. Gupta [10] reviewed different biometric authentication techniques for online voting systems and concluded that biometric verification significantly strengthens identity validation in digital elections.

S. Nakamoto [11] introduced the foundational concepts of blockchain technology and distributed systems, which established the principles of decentralized and tamper-proof transaction management used in modern blockchain applications, including e-voting systems. Y. Chen and H. Wang [12] focused on security analysis of smart contracts in Ethereum-based voting systems and highlighted

possible vulnerabilities such as reentrancy attacks and transaction manipulation. Their study emphasized the importance of secure smart contract development and proper testing practices.

Storage efficiency and scalability remain major concerns in blockchain-based voting systems. A. Joshi and M. Kulkarni [13] proposed a hybrid on-chain and off-chain storage model to reduce blockchain storage overhead while maintaining data integrity. Their research inspired the adoption of hybrid storage architectures in modern blockchain applications. D. Lee and J. Kim [14] discussed scalability challenges in blockchain-based e-voting systems and identified issues such as transaction latency, gas fees, and network congestion that affect large-scale deployment.

Recent studies have also explored transparency, governance, and decentralized application development in blockchain voting systems. M. Arora and S. Patil [15] presented a secure and transparent voting framework using blockchain technology and demonstrated how blockchain improves election auditability and reliability. V. Singh and P. Sharma [16] developed a blockchain-based decentralized application for online voting and highlighted the importance of distributed governance and accessibility in digital election systems.

N. K. Rao and A. Mishra [17] proposed an electronic voting system using blockchain and face recognition technology. Their work is closely related to the proposed system because it combines biometric authentication with decentralized vote storage. The study concluded that integrating blockchain with facial recognition improves election transparency and voter verification. S. Bhosale and R. Patil [18] worked on Ethereum smart contract optimization techniques for voting applications and suggested methods for reducing gas consumption and improving transaction efficiency.

Security and privacy challenges in decentralized voting systems have also been widely discussed in recent research. P. K. Sharma [19] analyzed security and privacy risks in blockchain-based voting systems and highlighted issues related to voter anonymity, cyberattacks, and data leakage. H. Lee [20] further examined cybersecurity risks in decentralized voting applications and emphasized the need for secure authentication mechanisms, encryption techniques, and infrastructure protection.

Recent advancements have also focused on scalability improvements and advanced authentication technologies. A. R. Khan and M. Ali [21] proposed blockchain-powered governance systems for secure digital administration and elections. R. Verma and S. Chauhan [22] discussed advanced face recognition techniques for secure authentication systems and recommended deep learning-based approaches for improving authentication accuracy and robustness. T. Joseph and K. Roy [23] introduced Layer-2 blockchain solutions to improve scalability and reduce transaction costs in blockchain-based voting systems.

The integration of blockchain and biometric technologies has received significant attention in recent years. M. Patel and J. Fernandes [24] discussed blockchain and biometric integration for digital elections and demonstrated that combining decentralized architectures with biometric authentication improves election integrity and transparency. Finally, S. Kulkarni and A. Patwardhan [25] explored the future scope of blockchain-based national voting systems and concluded that decentralized voting platforms have the potential to transform large-scale democratic processes through transparency, automation, and secure digital governance.

From the reviewed literature, it is clear that blockchain technology provides strong capabilities for building secure, transparent, and tamper-proof electronic voting systems. However, many existing systems still face challenges related to scalability, voter authentication, privacy, and storage efficiency. The proposed Decentralized E-Voting System addresses these limitations by integrating Ethereum blockchain, Solidity smart contracts, face recognition-based biometric authentication, and a hybrid on-chain/off-chain storage architecture to develop a secure, reliable, and scalable digital voting platform.

3. METHODOLOGY

The proposed Decentralized E-Voting System using Blockchain and Face Recognition follows a hybrid methodology that combines blockchain technology, biometric authentication, and web-based application development to create a secure and transparent voting platform. The methodology mainly focuses on improving election security, maintaining data integrity, preventing voter fraud, and reducing manual intervention during the voting process. The system integrates Ethereum blockchain, FastAPI backend services, face recognition techniques, and a web-based interface to build a decentralized voting environment.

The development process started with system planning and requirement analysis. During this stage, the major user roles were identified as Administrator, Voter, and Candidate. The administrator manages elections and verifies users, voters participate in elections after successful authentication, and candidates apply for elections and contest after approval. Different design models such as Data Flow Diagrams (DFD), UML diagrams, flowcharts, and system architecture diagrams were

prepared to define workflows and communication between system modules.

Blockchain technology acts as the core component of the proposed system. Ethereum blockchain was selected because of its decentralized structure and support for smart contracts. Smart contracts were developed using Solidity to automate important election activities including voter registration, candidate registration, election creation, vote casting, and result generation. Once deployed on the blockchain, these contracts automatically execute predefined rules and ensure that voting records cannot be modified. Each vote is stored as a blockchain transaction, which helps maintain transparency and immutability throughout the election process.

For development and testing, the blockchain network was deployed locally using Ganache, which provides a private Ethereum environment. MetaMask wallet integration was implemented for secure account management and transaction authorization. Communication between the backend and blockchain network was established using Web3.py, enabling interaction with deployed smart contracts and blockchain data.

The backend of the system was developed using FastAPI, a lightweight and high-performance Python framework. The backend handles API requests, user authentication, blockchain communication, and election-related operations. It also manages voter verification, candidate approval, election timelines, and duplicate voting prevention. SQLite database technology was used to store off-chain data such as user information, document references, and facial recognition data.

To strengthen authentication security, face recognition technology was integrated into the system. OpenCV was used for image processing and face detection. The Haar Cascade Classifier algorithm detects facial regions from uploaded images, while the Local Binary Pattern Histogram (LBPH) algorithm is used for face recognition. During the voting process, facial features captured from the user are compared with previously stored data to verify voter identity. This mechanism helps prevent impersonation and unauthorized voting.

The proposed system follows a hybrid storage architecture to improve scalability and reduce blockchain storage costs. Important election records such as votes, transaction hashes, and election details are stored on-chain, while large files including Aadhaar documents and facial images are maintained off-chain in the database. Cryptographic hashing techniques such as Keccak-256 are used to maintain integrity between on-chain and off-chain data.

The frontend of the application was developed using HTML, CSS, and JavaScript to provide a simple and user-friendly interface. Separate dashboards were designed for administrators, voters, and candidates. The frontend allows users to register, upload documents, complete authentication, participate in elections, and view election results in real time. REST APIs developed using FastAPI enable communication between frontend and backend modules.

The voting process follows a secure sequence of operations. Initially, voters register using their blockchain wallet address and upload identity documents along with facial images. After verification by the administrator, eligible users can participate in active elections. During voting, the system performs face recognition authentication before allowing vote casting. Once verified, the vote is recorded as an immutable blockchain transaction, and smart contracts automatically update vote counts and generate results in real time.

Testing and validation were conducted in a controlled environment to evaluate the functionality, performance, and security of the system. Different testing methods such as unit testing, integration testing, and system testing were performed on modules including registration, authentication, blockchain transactions, voting operations, and result generation. The results confirmed that the proposed system successfully prevents double voting, secures election records, and improves transparency in the election process.

The methodology used in this project demonstrates how blockchain technology and biometric authentication can be integrated to develop a secure and reliable decentralized voting platform. The proposed approach reduces the risk of election fraud, minimizes human intervention, and provides a scalable framework for future electronic voting systems.

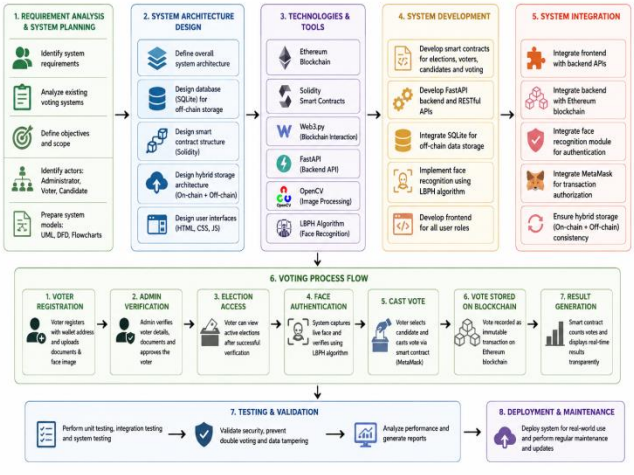

Fig -1: Methodology Diagram

4. IMPLEMENTATION DETAILS

The implementation of the proposed Decentralized E-Voting System using Blockchain and Face Recognition was carried out using blockchain technology, biometric authentication, backend frameworks, and web development technologies. The system was designed to provide secure election management, transparent vote recording, and reliable voter authentication through a decentralized architecture.

The implementation process began with the development of the blockchain layer using the Ethereum platform. Smart contracts were written in Solidity to manage important election operations such as voter registration, candidate registration, election creation, vote casting, and result generation. These smart contracts execute predefined election rules automatically without requiring manual intervention. Once deployed on the blockchain, the stored data becomes immutable, ensuring that voting records cannot be modified or tampered with.

For development and testing, the Ethereum blockchain was deployed locally using Ganache, which provides a private blockchain environment with test accounts and simulated transactions. MetaMask wallet integration was implemented to allow users to securely connect their Ethereum accounts and authorize blockchain transactions. Communication between the backend server and blockchain network was established using the Web3.py library, which enables interaction with deployed smart contracts and blockchain data retrieval.
The backend of the system was developed using the FastAPI framework in Python. FastAPI was selected because of its high performance and efficient API handling capabilities. The backend manages user authentication, election operations, blockchain communication, face recognition processing, and database management. REST APIs were developed for functionalities such as voter registration, candidate application, election creation, vote casting, and result retrieval.

SQLite database technology was used for storing off-chain information including voter details, candidate records, facial data, and document references. Since storing large files directly on the blockchain is expensive and inefficient, the system follows a hybrid storage architecture. Important election data and vote transactions are stored on-chain, while large files such as Aadhaar documents and facial images are maintained off-chain. Cryptographic hashing techniques are used to maintain integrity between blockchain records and off-chain data.

Biometric authentication was implemented using OpenCV and the Local Binary Pattern Histogram (LBPH) face recognition algorithm. During voter registration, users upload facial images that are processed and stored in the database. The Haar Cascade Classifier algorithm is used for face detection by identifying facial regions from uploaded images. The extracted facial features are then processed using the LBPH algorithm for voter verification.

During the voting process, the system captures or uploads a live facial image of the voter and compares it with previously stored facial data. If the similarity score matches the authentication threshold, the voter is allowed to cast a vote. This verification process helps prevent impersonation and unauthorized voting.

The frontend of the application was developed using HTML, CSS, and JavaScript. A responsive and user-friendly interface was designed for administrators, voters, and candidates. The frontend supports functionalities such as registration, document upload, election participation, face verification, candidate application, and real-time result viewing. JavaScript was used to manage dynamic interactions and API communication between frontend and backend services.

The administrator module allows authorized users to create elections, define election timelines, verify candidates and voters, and monitor election results. The voter module enables users to register, complete face authentication, upload identity documents, and cast votes securely. The candidate module allows users to apply for elections and wait for administrator approval before participation.

Several validation mechanisms were implemented to improve system security. Smart contracts verify whether a voter has already voted before allowing a new transaction. Backend validations ensure that only approved users can participate in active elections during the specified time period. MetaMask wallet authentication further improves transaction security and user verification.

The complete system was tested in a controlled local environment using the Ganache blockchain. Unit testing and integration testing were performed to validate functionalities such as registration, authentication, blockchain transactions, vote recording, and result generation. Experimental results confirmed that the system successfully improves transparency, prevents double voting, secures election records, and provides reliable biometric authentication.

The implementation demonstrates that combining blockchain technology with biometric verification can improve the security, transparency, and reliability of modern electronic voting systems. The developed framework also provides a practical foundation for future decentralized election platforms and can be extended

further using advanced blockchain networks and AI-based biometric authentication technologies.

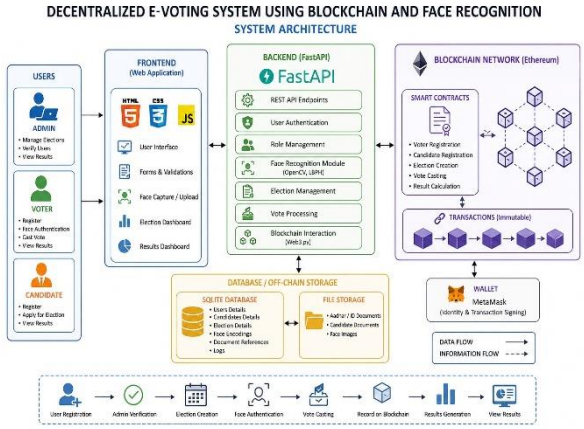

Fig -2: System Architecture Diagram

5. RESULTS AND DISCUSSION

The proposed Decentralized E-Voting System using Blockchain and Face Recognition was successfully implemented and tested in a controlled environment using Ethereum blockchain, Ganache, FastAPI, and OpenCV technologies. The system was evaluated on the basis of functionality, security, transparency, authentication accuracy, and overall system performance. The experimental results showed that the proposed framework effectively overcomes several limitations of traditional voting systems, including centralized control, vote tampering, impersonation, and manual vote counting.

The implementation results confirmed that the system successfully supports important functionalities such as voter registration, candidate registration, administrator verification, election creation, secure vote casting, and real-time result generation. The administrator module efficiently managed election activities by verifying users, controlling election timelines, and monitoring voting operations. The voter module allowed users to register securely using wallet-based authentication, upload identity documents, complete face verification, and cast votes through blockchain transactions. Similarly, the candidate module successfully handled candidate registration and approval processes.

The blockchain implementation ensured transparency and immutability throughout the election process. Each vote was stored as a blockchain transaction, making it impossible to modify voting records after submission. Smart contracts automatically enforced election rules such as preventing duplicate voting and restricting unauthorized access. The decentralized architecture removed dependence on a central authority and improved trust in the voting system.

The face recognition module showed satisfactory performance during testing. OpenCV-based face detection along with the LBPH face recognition algorithm successfully authenticated registered voters during the voting process. The system compared live facial images with previously stored data and allowed only verified users to participate in elections. However, testing also indicated that face recognition accuracy can be affected by factors such as lighting conditions and image quality.

Performance analysis showed that the FastAPI backend provided fast response times and smooth communication between the frontend, backend, and blockchain network. The REST API architecture efficiently handled user requests and election-related operations. Although blockchain transaction confirmation introduced slight delays, it ensured secure and tamper-proof vote recording. The hybrid storage architecture also improved system efficiency by storing only critical election data on-chain while maintaining large files such as facial images and identity documents off-chain.

The system implemented multiple security mechanisms to maintain election integrity. Blockchain technology provided transparent and immutable vote storage, while wallet-based authentication and biometric verification strengthened voter identity validation. The voting mechanism successfully prevented double voting by checking whether a voter had already participated before allowing a new transaction. Unauthorized users were restricted from accessing election functionalities without proper verification.

A comparison between the traditional voting system and the proposed decentralized system showed noticeable improvements in transparency, automation, security, and fraud prevention. Unlike traditional systems that rely on centralized management and manual vote counting, the proposed system automated election operations using smart contracts and generated results in real time. The use of biometric authentication further improved reliability by reducing impersonation risks.

Despite the successful implementation, some limitations were identified during testing. The system currently operates on a local blockchain network using Ganache, which limits scalability for large-scale deployment. Blockchain transactions may also introduce latency when handling many users simultaneously. In addition, the existing face recognition module remains vulnerable to spoofing attacks using photographs because liveness detection mechanisms are not yet implemented. Managing

blockchain wallet credentials may also be challenging for non-technical users.

Overall, the results confirm that integrating blockchain technology with biometric authentication provides a secure, transparent, and efficient framework for modern electronic voting systems. The proposed system demonstrates the practical feasibility of decentralized digital voting and establishes a strong foundation for future improvements and real-world deployment.

6. FUTURE SCOPE

The proposed decentralized e-voting system can be further improved by integrating advanced technologies to enhance security, scalability, and practical usability. One possible improvement is the use of advanced deep learning-based face recognition models such as FaceNet, DeepFace, and Dlib, which can provide better accuracy and more reliable authentication under different lighting and environmental conditions. In addition, liveness detection techniques such as blink detection, head movement analysis, and real-time video verification can be implemented to reduce the risk of spoofing attacks using photographs or recorded videos.

The security of the system can also be strengthened by implementing end-to-end encryption, secure key management techniques, and direct MetaMask transaction signing without exposing private keys to the backend server. These measures can improve transaction safety and protect sensitive user information.
For large-scale real-world deployment, the system can be extended by deploying it on public blockchain networks such as Ethereum Mainnet or Polygon instead of a local Ganache environment. Layer-2 blockchain solutions can also be integrated to reduce gas fees and improve transaction speed and scalability when handling a large number of voters simultaneously.

In the future, mobile application support for Android and iOS platforms can be developed to increase accessibility and improve voter participation. Integration with national digital identity systems and cloud-based infrastructure can further enhance reliability, usability, and adoption of the system for government, organizational, and institutional elections. These improvements can help transform the proposed framework into a more practical and scalable next-generation digital voting solution.

7. CONCLUSIONS

The proposed Decentralized E-Voting System using Blockchain and Face Recognition successfully demonstrates a secure, transparent, and efficient digital voting platform that addresses several limitations of traditional voting systems, including centralized control, vote tampering, impersonation, and lack of transparency. By integrating Ethereum blockchain technology with Solidity smart contracts, the system ensures secure and immutable vote recording while automating important election operations such as voter registration, candidate verification, vote casting, and result generation.

The integration of biometric authentication using OpenCV and the LBPH face recognition algorithm improves voter verification and helps prevent unauthorized voting. In addition, the hybrid storage architecture increases system efficiency by storing critical election data on the blockchain while maintaining large files such as facial images and identity documents off-chain.

The experimental results confirmed that the system successfully improves transparency, prevents double voting, strengthens election security, and reduces manual intervention during the voting process. The decentralized architecture also increases trust in the election process by ensuring that voting records cannot be altered after submission.

Although certain challenges such as blockchain scalability, transaction latency, and face spoofing risks still remain, the project provides a strong foundation for future decentralized voting systems. Overall, the study demonstrates that combining blockchain technology with biometric authentication can significantly improve the security, reliability, and trustworthiness of modern electronic voting systems.

REFERENCES

[1] M. M. H. Onik, M. A. R. Ahad, S. M. S. Hossain, and M. R. K. Alam, “Blockchain in the Era of Industry 4.0: A Review on E-Voting System,” IEEE Access, vol. 9, pp. 122–145, 2021.

[2] A. K. Singh and R. Kumar, “Blockchain-Based Electronic Voting System: A Review,” International Journal of Advanced Computer Science and Applications, vol. 13, no. 2, pp. 234–240, 2022.

[3] S. Pawar and R. Sharma, “Secure Blockchain-Based Electronic Voting Using Smart Contracts,” International Journal of Computer Applications, vol.

184, no. 12, pp. 15–21, 2022.

[4] H. Patel and D. Shah, "Decentralized Voting System using Ethereum Blockchain," International Journal of Innovative Research in Technology, vol. 9, no. 5, pp. 101–107, 2022.

[5] P. Sharma and A. Verma, "Blockchain-Based Secure Voting System with Biometric Authentication," Journal of Information Security and Applications, vol. 68, pp. 1–10, 2023.

[6] M. Gupta and S. Jain, "Implementation of Smart Contract-Based E-Voting System," International Journal of Engineering Research & Technology, vol. 12, no. 4, pp. 201–207, 2023.

[7] K. Rathi and V. Kulkarni, "Blockchain-Powered Transparent Voting Mechanism," Procedia Computer Science, vol. 218, pp. 115–123, 2023.

[8] T. Nguyen and L. Tran, "A Secure E-Voting Framework Using Ethereum Blockchain," IEEE International Conference on Blockchain Computing and Applications, pp. 220–227, 2023.

[9] R. Mehta and P. Deshmukh, "Face Recognition-Based Authentication for Secure Voting Systems," International Journal of Computer Vision and Image Processing, vol. 13, no. 3, pp. 55–67, 2023.

[10] R. Gupta, "Biometric Authentication Techniques for Online Voting," Journal of Emerging Technologies and Innovative Research, vol. 10, no. 6, pp. 402–409, 2023.

[11] S. Nakamoto, "Blockchain Technology and Secure Distributed Systems," Blockchain Research Journal, vol. 5, no. 1, pp. 1–15, 2020.

[12] Y. Chen and H. Wang, "Smart Contract Security Analysis in Ethereum-Based Voting Systems," IEEE Access, vol. 11, pp. 55410–55425, 2023.

[13] A. Joshi and M. Kulkarni, "Hybrid On-chain and Off-chain Storage Model for Blockchain Applications," International Journal of Advanced Research in Computer Science, vol. 14, no. 2, pp. 77–85, 2023.

[14] D. Lee and J. Kim, "Scalability Challenges in Blockchain-Based E-Voting Systems," IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 3300–3312, 2024.

[15] M. Arora and S. Patil, "Secure and Transparent Voting using Blockchain Technology," International Conference on Emerging Technologies in Computer Engineering, pp. 89–96, 2024.

[16] V. Singh and P. Sharma, "Blockchain-Based Decentralized Application for Online Voting," International Journal of Scientific Research in Engineering and Management, vol. 8, no. 1, pp. 45–52, 2024.

[17] N. K. Rao and A. Mishra, "Electronic Voting System Using Blockchain and Face Recognition," International Journal of Computer Science and Mobile Computing, vol. 13, no. 4, pp. 120–128, 2024.

[18] S. Bhosale and R. Patil, "Ethereum Smart Contract Optimization for Voting Applications," Journal of Blockchain Technology, vol. 6, no. 2, pp. 66–74, 2024.

[19] P. K. Sharma, "Security and Privacy Challenges in Blockchain-Based Voting," IEEE International Conference on Cyber Security and Protection of Digital Services, pp. 188–194, 2024.

[20] H. Lee, "Cybersecurity Risks in Decentralized Voting Applications," International Journal of Network Security, vol. 27, no. 1, pp. 90–101, 2025.

[21] A. R. Khan and M. Ali, "Blockchain-Powered Secure Governance Systems," International Journal of Information Technology, vol. 16, no. 2, pp. 300–309, 2025.

[22] R. Verma and S. Chauhan, "Advanced Face Recognition Techniques for Secure Authentication," Journal of Artificial Intelligence and Data Science, vol. 4, no. 1, pp. 55–66, 2025.

[23] T. Joseph and K. Roy, "Layer-2 Blockchain Solutions for Scalable E-Voting Systems," IEEE Access, vol. 13, pp. 10210–10224, 2025.

[24] M. Patel and J. Fernandes, "Blockchain and Biometric Integration for Digital Elections," Journal of Computer Engineering and Applications, vol. 15, no. 3, pp. 144–153, 2026.

[25] S. Kulkarni and A. Patwardhan, "Future Scope of Blockchain-Based National Voting Systems," International Journal of Advanced Computing and Communication Technologies, vol. 14, no. 1, pp. 10–21, 2026.