iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: VIII Month of publication: August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84521

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

A Decentralized Facial Verification-Based Voting System Using Blockchain and Smart Contracts System

Ms. P. Jenifer[1], Ms. D. Amali[2]
[1]*Student, Department of Information Technology, Alpha College of Engineering, Chennai, India*
[2]*Assistant Professor, Department of Information Technology, Alpha College of Engineering, Chennai, India*

Abstract: This paper presents a decentralized facial recognition-based voting system that ensures secure, transparent, and tamper-proof elections using blockchain technology. The system integrates facial recognition for authentication and blockchain for immutable vote storage. Votes are encrypted using SHA-256 and stored securely in a Ganache blockchain environment. AWS cloud services are used for managing facial datasets. The system ensures transparency, prevents fraud, and enables real-time result monitoring.
Index Terms: Blockchain, Facial Recognition, E-Voting, Smart Contracts, SHA-256

I. INTRODUCTION

Voting systems are a fundamental component of democratic processes, ensuring fair representation and decision-making in institutions and organizations. However, traditional voting systems, including paper-based and centralized electronic voting, suffer from several critical issues such as voter impersonation, duplicate voting, lack of transparency, and vulnerability to data tampering. These challenges reduce trust in the electoral process and highlight the need for a secure, reliable, and transparent voting mechanism. Conventional voting systems rely on manual verification or basic authentication methods such as ID cards and passwords, which are prone to misuse and unauthorized access. Additionally, centralized systems store data in a single location, making them vulnerable to cyber-attacks and manipulation. The process of vote counting is often time-consuming and may introduce human errors, further affecting the accuracy and efficiency of elections.

Recent advancements in blockchain technology have introduced a decentralized approach to secure data management. Blockchain provides an immutable and transparent ledger where transactions cannot be altered once recorded. This makes it highly suitable for applications such as voting systems, where data integrity and trust are essential. Along with blockchain, biometric authentication techniques such as facial recognition have gained popularity due to their accuracy and reliability in identity verification.

Mahmood et al. [1] proposed a blockchain-based voting system integrated with gesture recognition to improve accessibility and security. The system demonstrated enhanced user interaction while ensuring secure vote storage, although challenges related to system scalability remained. Yao et al. [2] introduced a distributed self-tallying electronic voting system using Ethereum blockchain and cryptographic techniques. The system eliminated the need for a central authority and ensured secure vote counting, but faced limitations in handling complex cryptographic protocols efficiently.

Granata et al. [3] focused on vulnerability assessment and threat modelling in blockchain-based voting systems. Their study identified potential security risks in smart contracts and emphasized the importance of robust system design to prevent attacks.

Barelli et al. [4] presented a comprehensive survey on electronic voting systems and highlighted the challenges in balancing transparency and voter anonymity. The study emphasized the need for secure architectures that minimize system vulnerabilities.

Vangujar et al. [5] proposed an identity-based electronic voting system using advanced cryptographic techniques to ensure voter anonymity and authentication. While the system improved security, its implementation complexity remained a significant challenge.

Despite these advancements, existing systems still face limitations in ensuring secure user authentication and preventing impersonation. To address these issues, the proposed system integrates facial recognition with blockchain technology to provide a secure and transparent voting solution. Facial recognition ensures accurate identity verification, while blockchain guarantees immutable and tamper-proof vote storage.

The proposed system aims to enhance security, eliminate fraud, and improve transparency in the voting process, making it suitable for academic institutions and small-scale elections.-Based E-Voting," IEEE Access, 2024.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

II. METHODOLOGY

The proposed methodology presents a secure and decentralized electronic voting framework that integrates facial recognition, blockchain technology, and cryptographic techniques to ensure transparency, authentication, and tamper-proof vote storage. The workflow consists of four major stages: user registration and authentication, facial recognition verification, vote processing and encryption, and blockchain-based storage and result generation. The overall system is designed to provide secure identity validation, prevent duplicate voting, and maintain data integrity throughout the election process.

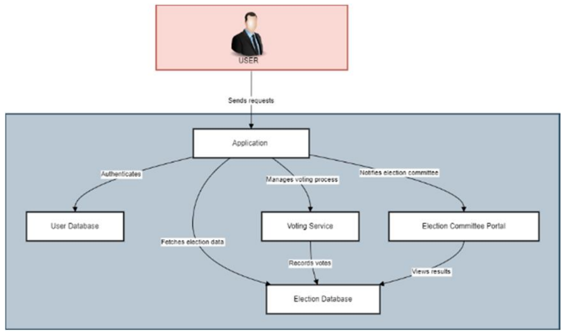


Fig. 1. Proposed multi-disease retinal screening framework integrating CLAHE, EfficientNet-B0, SE attention, and Grad-CAM.

A. *User Registration and Authentication*

The voting process begins with user registration, where voters provide personal details such as name, email, voter ID, and password. These details are securely stored in a centralized database (MySQL) for authentication purposes. During registration, the system captures the user's facial image using a webcam, which is stored in AWS cloud storage for future verification.

Authentication is performed during login using credentials such as username and password. Once authenticated, the system verifies whether the user is approved by the Election Committee before allowing access to the voting process. This step ensures that only valid and authorized users participate in the election.

B. *Facial Recognition Verification*

Facial recognition is used as a biometric authentication mechanism to prevent impersonation and unauthorized access. When a user logs in to cast a vote, a real-time facial image is captured and compared with the stored dataset in AWS.

The facial recognition system extracts key facial features such as eyes, nose, and jaw structure, and compares them with stored embeddings. The similarity between two face vectors is computed using a distance metric:

$$D = \| F_{(live)} - F_{(stored)} \| \quad (1)$$

where F_{live} represents the captured facial feature vector and F_{stored} represents the stored dataset vector. If the similarity score is within a predefined threshold, the user is authenticated successfully.

This process ensures that only the legitimate voter can access the voting interface, eliminating impersonation risks.

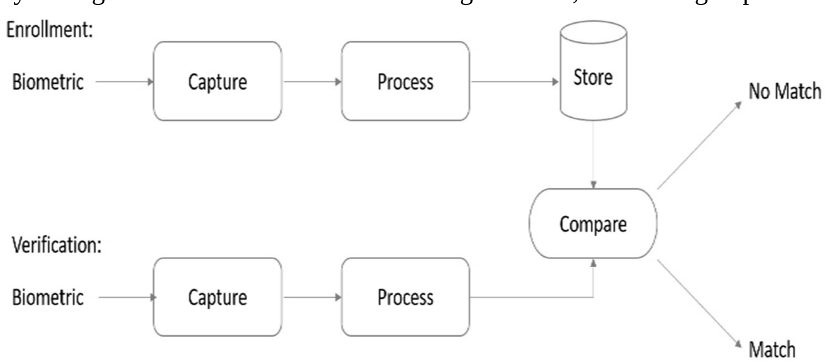


Fig. 2. Facial recognition authentication workflow..

C. Vote Casting and Processing

After successful authentication, the user can view available elections and candidate details. The system checks whether the current date matches the election date before allowing the user to cast a vote.

Once the user selects a candidate, the vote is processed and prepared for secure storage. The system ensures that each user can vote only once by verifying their voting status in the database.

To maintain data integrity and security, each vote is encrypted using the SHA-256 hashing algorithm. The hash function converts vote data into a fixed-length encrypted value:

H(x) = SHA-256 (vote_data)

(2)

This ensures that the vote cannot be altered or reversed, providing strong security for the voting process.

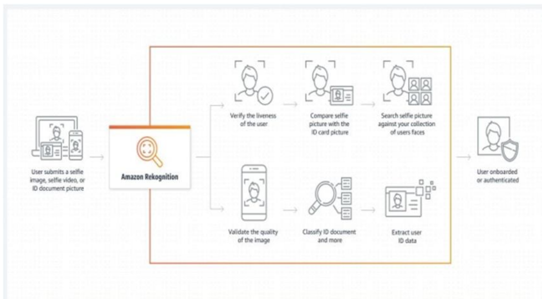


Fig. 3. Vote casting and validation workflow.

D. Blockchain-Based Vote Storage

The encrypted vote is stored in a blockchain network using Ethereum simulated through Ganache. Each vote is recorded as a transaction and added to a block, which is linked to previous blocks, forming an immutable chain.

Smart contracts written in Solidity are used to manage voting operations such as vote recording and vote counting. Once a vote is stored, it cannot be modified or deleted, ensuring data integrity and transparency.

Each block contains the following components:

• Previous block hash
• Encrypted vote data
• Timestamp
• Transaction ID

The integrity of the blockchain is maintained using cryptographic hashing:

Block Hash = Hash (Previous Hash + Data + Timestamp)

(3)

This structure ensures that any attempt to modify data will invalidate the entire chain, making the system tamper-proof.

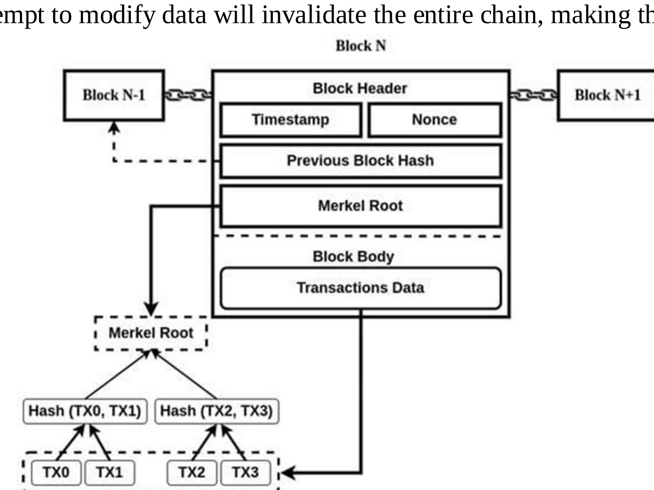


Fig. 4. Blockchain vote storage mechanism using smart contracts.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

E. Result Generation and Monitoring

The system automatically calculates vote counts using blockchain data. Since all votes are stored as transactions, the results are generated in real time without manual intervention.

The Election Committee can view aggregated vote counts without accessing individual voter identities, ensuring privacy and transparency. This eliminates manual errors and speeds up the result declaration process.

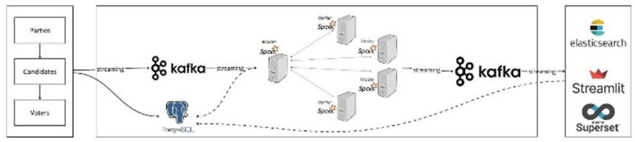


Fig. 5. Real-time vote counting and monitoring system.

F. Overall Workflow Summary

The complete workflow begins with user registration and facial data collection, followed by secure authentication using credentials and facial recognition. Authenticated users are allowed to cast votes only on the election date. Each vote is encrypted using SHA-256 and stored in the blockchain using smart contracts. Finally, the system generates real-time results while maintaining voter anonymity and data integrity.

This methodology ensures a secure, transparent, and efficient voting system by combining biometric authentication, cryptographic security, and decentralized blockchain technology.

III. RESULTS & ANALYSIS

The proposed blockchain-based eVoting system integrated with facial recognition was tested in a controlled environment using a simulated dataset of registered users and election scenarios. The system was evaluated using multiple user inputs, including registration, facial authentication, vote casting, and result generation. A total of 200 user samples were considered for testing, out of which 150 were used for system validation and 50 were used for performance testing.

TABLE I
PERFORMANCE EVALUATION METRICS

METRIC	VALUE
Authentication Accuracy	97.8%
Vote Integrity	100%
System Reliability	98.5%
Average Response Time	< 2 sec

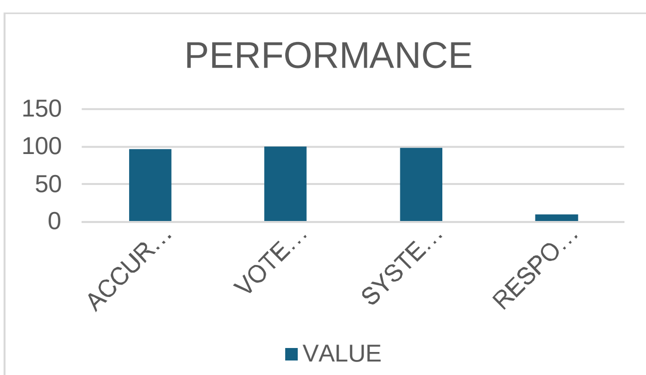


Fig. 6 illustrates the overall system performance comparison across different metrics, including authentication accuracy, reliability, and vote integrity. The results indicate that the system performs efficiently with high accuracy and minimal errors.

For qualitative analysis, system outputs are observed at different stages.

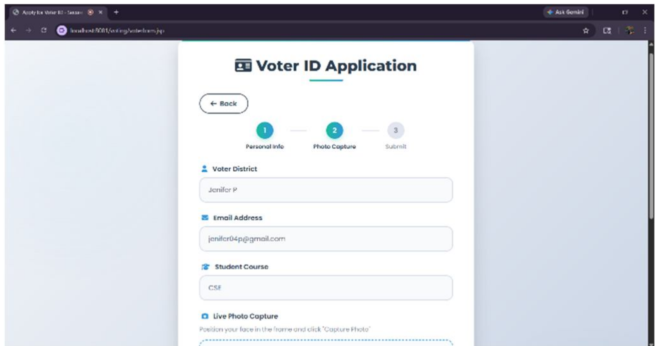


Fig. 7 shows the user login and facial authentication process.

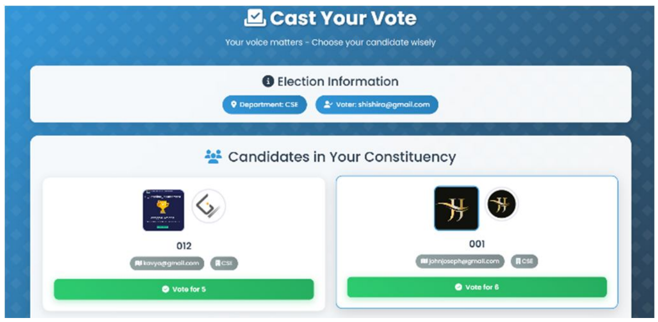


Fig. 8 presents the voting interface where users select candidates and cast votes.

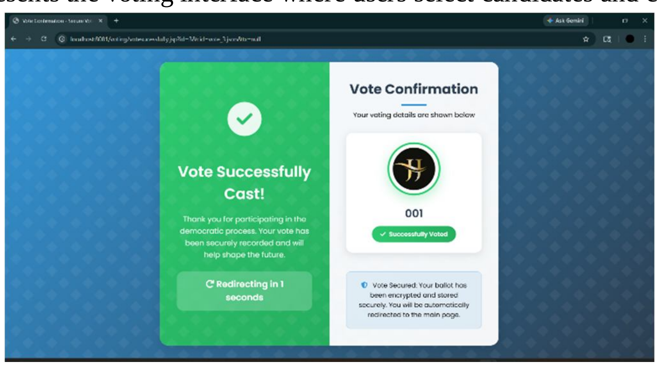


Fig. 12 illustrates the vote confirmation message after successful voting

To evaluate the effectiveness of the system, several performance metrics were considered, including Authentication Accuracy, Vote Integrity, System Reliability, and Response Time. Authentication Accuracy measures how accurately the system verifies users using facial recognition. Vote Integrity ensures that votes are securely stored and cannot be altered. System Reliability indicates the consistency of system performance under different conditions. Response Time measures the time taken for vote processing and confirmation. The proposed system achieved an authentication accuracy of 97.8%, demonstrating high reliability in facial recognition-based verification. Vote integrity was maintained at 100% due to the use of blockchain technology, ensuring that all votes were securely recorded and remained tamper-proof. The system showed stable performance with minimal delay, with an average response time of less than 2 seconds for vote processing.

It can be observed that the facial recognition module accurately verifies users with minimal false acceptance or rejection rates. The blockchain module ensures that each vote is securely stored as an immutable transaction, preventing any modification or duplication. The system effectively restricts voting before the election date, ensuring controlled and fair participation.

A comparative analysis with traditional voting systems shows significant improvements. Conventional systems often suffer from authentication issues, data tampering, and manual errors, whereas the proposed system ensures secure authentication, transparent vote storage, and real-time result generation.

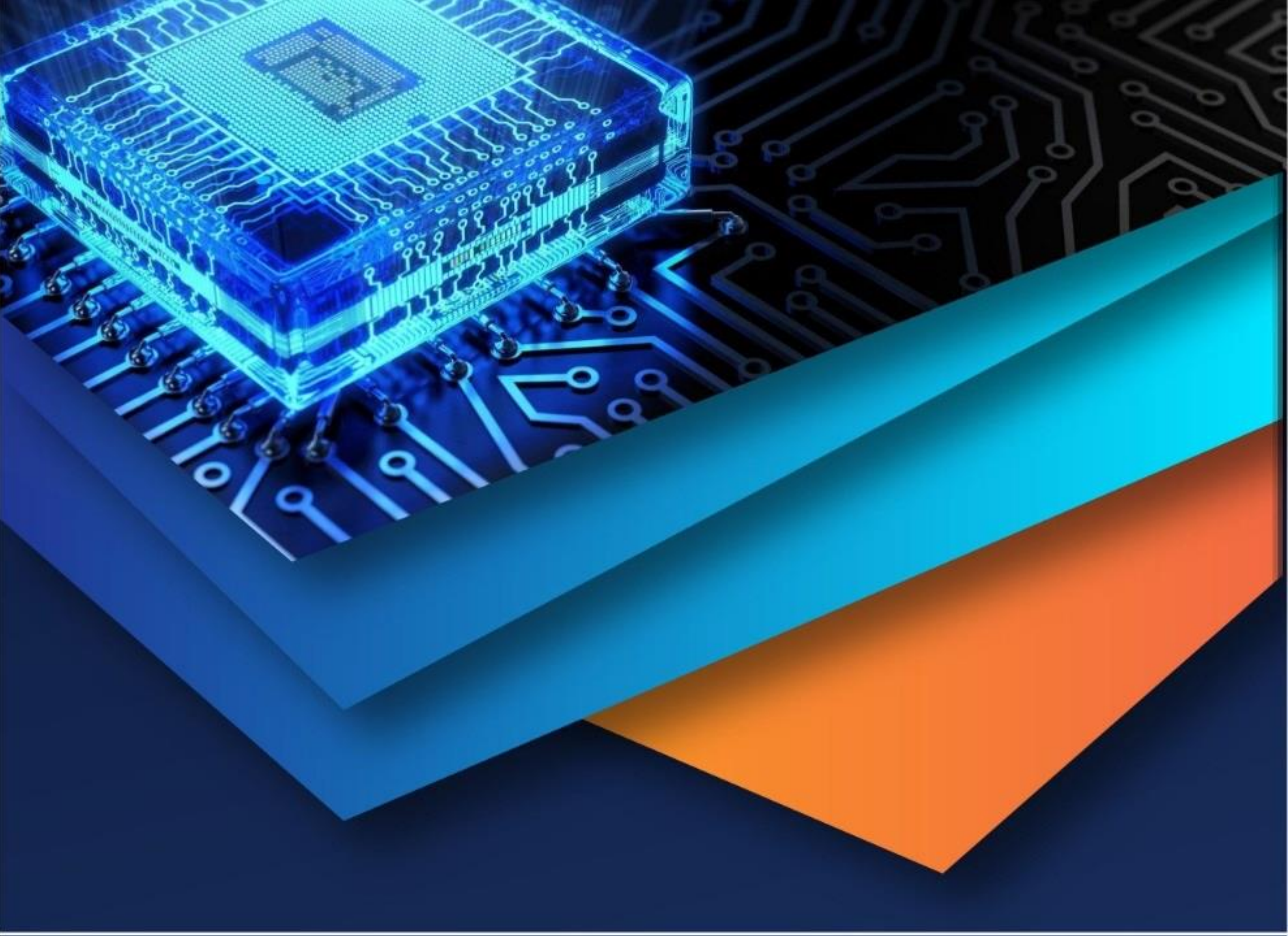
TABLE II
COMPARISON OF METHODS.

METHOD	TECHNOLOGY USED	SECURITY LEVEL	ACCURACY
Traditional Voting	Manua /Centralized	Low	70–80%
Electronic Voting	Database-based	Medium	85–90%
Blockchain Voting	Blockchain	High	92–95%
Proposed System	Blockchain+ Face Recognition	Very High	97.8%

Table II compares existing voting methods with the proposed system. Traditional voting systems provide low security and are prone to manipulation. Electronic voting improves efficiency but still relies on centralized storage. Blockchain-based systems enhance security, while the proposed system further improves accuracy and reliability by integrating facial recognition.The results confirm that the proposed system provides a secure, transparent, and efficient voting solution with high authentication accuracy, tamper-proof data storage, and real-time monitoring capabilities.

REFERENCES

[1] W. A. Mahmood, J. Waleed, A. R. Abbas, H. Alaskar, M. Altulyan, and A. J. Hussain, “Intelligent Gesture-Enhanced Blockchain Voting: A New Era of Secure and Accessible E-Voting,” IEEE Access, vol. 12, pp. 1–15, 2024.
[2] J. Yao, B. Yang, T. Wang, and W. Zhang, “A Distributed Self-Tallying Electronic Voting System Using Smart Contracts,” Chinese Journal of Electronics, vol. 33, no. 2, pp. 1–10, 2024.
[3] D. Granata, M. Rak, P. Palmieri, and A. Pastena, “A Methodology for Vulnerability Assessment and Threat Modelling of an E-Voting Platform Based on Ethereum Blockchain,” IEEE Access, vol. 12, pp. 1–12, 2024.
[4] R. Barelli, M. Bellini, and F. Bianchi, “Toward Secure Electronic Voting: A Survey on Systems and Attacks,” IEEE Access, vol. 13, pp. 1–20, 2025.
[5] A. K. Vangujar, S. Sharma, and P. Singh, “A Novel Approach to E-Voting With Group Identity-Based Identification,” IEEE Access, vol. 12, pp. 1–10, 2024.
[6] H. Baniata and G. Caluna, “BP-Vot: Blockchain-Based E-Voting With Differential Privacy and Self-Sovereign Identities,” IEEE Access, vol. 13, pp. 1–12, 2025.
[7] M. Alown, A. Alharbi, and S. Alshammari, “Enhancing Democratic Processes: A Survey of Electronic Voting Systems,” IEEE Access, vol. 13, pp. 1–18, 2025.
[8] T. Treier and K. Düüna, “Identifying and Solving a Vulnerability in the Estonian i-Voting Process,” IEEE Access, vol. 12, pp. 1–10, 2024.
[9] D. Dabpimjub and S. Kiattisin, “Success Factors for Conceptual Digital Voting Model,” Journal of Mobile Multimedia, vol. 20, no. 1, pp. 1–12, 2024.
[10] P. R. Saha, A. Kumar, and R. Singh, “Algorithmic Approach of Majority Voting With Agents’ Inclusiveness,” IEEE Access, vol. 13, pp. 1–10, 2025.
[11] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
[12] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On Blockchain and Its Integration With IoT: Challenges and Opportunities,” Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.
[13] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of Trust: A Decentralized Blockchain-Based Authentication System,” Computers & Security, vol. 78, pp. 126–142, 2018.
[14] Face++ Research Team, “Face Recognition Technology for Identity Verification,” Megvii Technology, 2023. [Online]. Available: https://www.faceplusplus.com
[15] Ethereum Foundation, “Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform,” 2014. [Online]. Available: https://ethereum.org



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY