International Conference on Science, Engineering & Management Trends

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Decentralized Voting Using Face Recognition and Blockchain

Sneha Baby K X, Ms. Sherine Sebastian
Department of Computer Science Engineering Rajagiri School of Engineering and Technology Kochi, India

Abstract- Electronic voting systems have gained significant importance in modern democratic processes; however, ensuring security, transparency, and voter authenticity remains a major challenge. This paper proposes a secure and decentralized e-voting system that integrates face recognition technology with blockchain. The face recognition module is used for biometric authentication, ensuring that only legitimate users can participate in the voting process. The blockchain technology is utilized to store votes in a tamper-proof and immutable manner using smart contracts. The system follows a structured workflow consisting of user registration, authentication, vote casting, and blockchain-based storage. Each vote is recorded as a transaction in the blockchain, ensuring transparency and eliminating the risk of data manipu-lation. The integration of MetaMask and Ganache enables secure transaction handling and efficient testing of the system. The proposed approach enhances the reliability and trustwor-thiness of the voting system by preventing unauthorized access, duplicate voting, and vote tampering. The system provides a scalable and secure solution for modern electronic voting appli-cations and demonstrates the potential of combining biometric authentication with decentralized technologies.

Keywords- E-Voting, Blockchain, Face Recognition, Smart Contracts, Biometric Authentication, Ethereum, Security

I. INTRODUCTION

In a democratic nation, voting plays a vital role in determin-ing the governing body by allowing citizens to express their choices freely. Traditional voting methods, whether paper-based or electronic, often encounter issues such as vote tampering, unauthorized access, and a lack of transparency in vote counting. These problems undermine public trust in the electoral process and raise serious concerns regarding the security and integrity of elections.

With the advancement of technology, researchers and gov-ernments have begun exploring modern solutions to make the voting process more secure, transparent, and efficient. Among these technologies, blockchain has emerged as a powerful solution due to its decentralized and tamper-resistant nature. Blockchain provides an immutable ledger in which every transaction (vote) is permanently recorded and can be verified by all participants without relying on a central authority. This ensures transparency, auditability, and strong resistance to data manipulation.

However, ensuring security in voting systems is not limited to protecting data alone; it also involves verifying that each voter is legitimate and unique. To address this challenge, bio-metric authentication techniques such as face recognition have gained significant importance. Face recognition technology

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

verifies a voter's identity based on facial features, thereby preventing impersonation and multiple voting attempts. Fur-thermore, the inclusion of a One-Time Password (OTP) veri-fication step adds an additional layer of security, resulting in a robust multi-factor authentication mechanism.

The integration of blockchain, face recognition, and OTP verification creates a reliable and secure framework for elec-tronic voting systems. This approach minimizes human in-tervention while enhancing transparency, accuracy, and effi-ciency. It also enables secure remote voting, ensuring both the confidentiality and integrity of the voting process.

In this paper, a blockchain-based e-voting system integrated with face recognition and OTP authentication is proposed. The primary objective is to develop a modern, secure, and transparent voting mechanism that overcomes the limitations of traditional systems and strengthens trust among voters and election authorities.

II. RELATED WORK

Electronic voting (e-voting) systems have gained significant attention in recent years due to the need for secure, transparent, and efficient electoral processes. Traditional voting systems suffer from issues such as vote tampering, lack of transparency, and centralized control, which have motivated researchers to explore advanced technologies such as blockchain and biometric authentication.

Blockchain technology has emerged as a promising solution for secure e-voting due to its decentralized and immutable nature. A blockchain-based e-voting system integrated with face recognition was proposed in [1], where the authors demonstrated how blockchain ensures secure vote storage while facial recognition is used for voter authentication. Simi-larly, the work presented in [2] focused on improving electoral integrity and accessibility by combining blockchain with facial recognition techniques. Their system highlighted the benefits of transparency and tamper-resistance in voting systems.

Biometric authentication has also been widely used to ensure voter identity and prevent impersonation. A secure online voting system using biometric authentication along with blockchain was introduced in [3], emphasizing the importance of identity verification in reducing fraudulent activities. In another study [4], the integration of face recognition with blockchain technology was explored, showing that biometric-based systems can significantly enhance the security of e-voting systems by ensuring that only legitimate users can cast votes.

To further strengthen security, multi-factor authentication mechanisms have been proposed. A smart voting system incor-porating face detection, OTP verification, and blockchain was presented in [5]. This approach combines biometric authen-tication with OTP-based verification, providing an additional layer of security and reducing the chances of unauthorized access. Such systems demonstrate the effectiveness of com-bining multiple authentication techniques to enhance system robustness.

In addition to authentication, several researchers have fo-cused on improving the underlying blockchain protocols used in voting systems. A traceable self-tallying e-voting protocol was introduced in [6], which allows voters to verify the correctness of election results without compromising privacy. A framework for improving transparency using blockchain was proposed in [7], highlighting the importance of decentralized systems in eliminating the need for a central authority. Further-more, an improved secure and efficient e-voting scheme was presented in [9], addressing challenges related to scalability and performance in blockchain-based voting systems.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Privacy preservation and voter anonymity are also critical aspects of e-voting systems. A blockchain-based voting system ensuring anonymity and verifiability was discussed in [11], where cryptographic techniques were used to protect voter identity. Similarly, privacy-preserving e-voting systems using biometrics and blockchain were proposed in [17], focusing on maintaining a balance between security and user privacy. A decentralized self-tallying voting protocol suitable for large-scale elections was introduced in [18], demonstrating the feasibility of implementing secure voting systems at a national level.

Several review-based studies have analyzed the challenges and solutions in blockchain-based voting systems. Comprehen-sive reviews of decentralized voting systems and their limita-tions were provided in [13] and [14], discussing issues such as scalability, security, and implementation complexity. The role of biometric authentication in enhancing voter verification was emphasized in [8] and [12], highlighting its importance in ensuring voter uniqueness and preventing duplicate voting.

Despite these advancements, existing systems often focus on individual aspects such as blockchain or biometric authen-tication, with limited integration of multiple security mech-anisms. Moreover, challenges such as scalability, transaction latency, and real-time authentication still remain. Therefore, the proposed system aims to overcome these limitations by integrating blockchain technology with face recognition and OTP-based multi-factor authentication to provide a more se-cure, transparent, and efficient e-voting solution.

III. METHODOLOGY

A. System Overview

The proposed system is a secure and decentralized elec-tronic voting platform that integrates biometric authentication using face recognition with blockchain technology for secure vote management. The primary objective of the system is to ensure that only legitimate users are allowed to cast votes while maintaining the integrity, transparency, and immutability of the voting process.

The system operates in multiple stages, including user reg-istration, authentication, vote casting, and vote storage. During the registration phase, users provide their identity details along with facial data, which is stored in the system as a reference for future verification. In the authentication phase, the system captures the live facial image of the user and verifies it against the stored data to confirm identity.

Once authenticated, the user is allowed to cast a vote through a user-friendly interface. The vote is then securely transmitted to the blockchain network, where it is recorded as a transaction using smart contracts. The decentralized nature of blockchain ensures that the voting data is distributed across multiple nodes, eliminating the risk of centralized tampering or data manipulation.
The system is designed to support transparency and trust by allowing verification of votes without revealing voter identity. By combining biometric verification with blockchain storage, the proposed approach addresses major challenges in tradi-tional voting systems such as impersonation, vote duplication, and data tampering.

B. Face Recognition Module

The face recognition module plays a crucial role in ensuring secure and reliable user authentication. This module is respon-sible for detecting, extracting, and verifying facial features of users during both registration and login phases. The system utilizes a real-time video stream captured through a webcam to perform face detection and recognition.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

Initially, the input video is divided into frames, and each frame is processed to detect the presence of a human face using a Single Shot Detector (SSD) model. The SSD model is efficient for real-time applications as it performs object detection in a single forward pass, enabling fast and accurate face localization.

After detecting the face, the region of interest (ROI) is extracted and passed through a feature extraction model. This model analyzes unique facial characteristics such as the distance between eyes, nose shape, jawline structure, and other distinguishing features. These features are then converted into a numerical representation known as a face embedding or feature vector.

During the registration phase, the extracted feature vector is stored in the system database as a reference template for the user. During authentication, a new feature vector is generated from the live input and compared with the stored template using similarity measurement techniques such as Euclidean distance or cosine similarity.

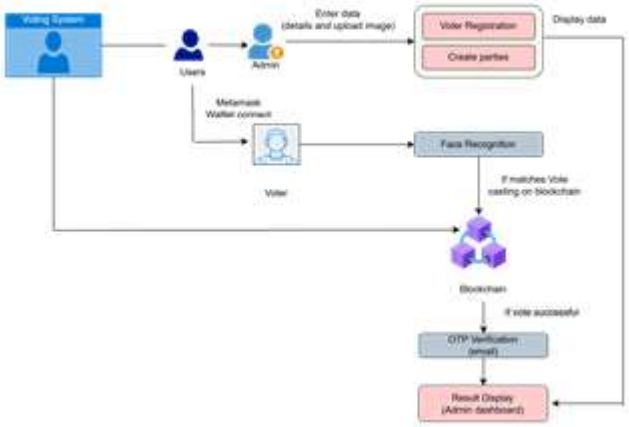

Fig. 1. System Architecture of the Proposed E-Voting Framework

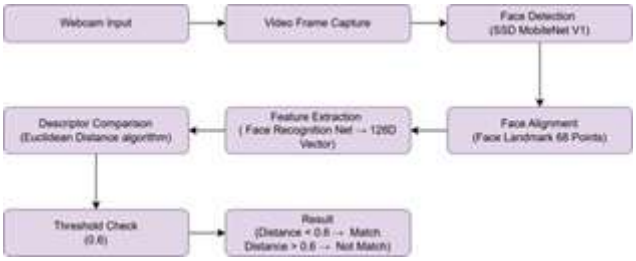

Fig. 2. Block diagram of Face Recognition

The matching process is mathematically represented as:

$$d = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \qquad (1)$$

where xi represents the stored feature vector and yi rep-resents the input feature vector. If the computed distance is below a predefined threshold, the system considers the match successful and grants access to the user.

This module ensures high accuracy and security by pre-venting unauthorized access and impersonation. Additionally, real-time processing enables seamless user experience without noticeable delays. The integration of face recognition signifi-cantly enhances the reliability of the voting system by ensuring that each vote is cast only by the legitimate voter.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

C. User Authentication Process

The user authentication process ensures that only authorized individuals are allowed to participate in the voting system. It consists of two main phases: registration and login. During the registration phase, users are required to provide their personal details along with their facial data. The system captures multiple facial samples using a webcam to improve recognition accuracy and generates corresponding feature vectors, which are securely stored for future verification.

During the login phase, the system captures a live video stream of the user and extracts the facial features using the face recognition module. The generated feature vector is then compared with the stored reference vectors associated with the registered user. If the similarity score satisfies the predefined threshold, the user is successfully authenticated.

To enhance security, the system ensures liveness detection by verifying that the input is from a real person rather than a static image or video replay. This prevents spoofing attacks and unauthorized access. Additionally, the system restricts multiple voting attempts by maintaining a record of users who have already cast their votes. Once a user is authenticated and marked as having voted, further attempts are denied.

This authentication mechanism provides a robust and re-liable approach by combining biometric verification with system-level constraints, thereby ensuring that each vote is cast only once by a legitimate voter.

D. Blockchain Module

The blockchain module is responsible for securely storing voting data in a decentralized and tamper-proof manner. The system utilizes Ethereum blockchain technology, where each vote is recorded as a transaction within a block. Smart con-tracts written in Solidity are deployed to define and manage the voting logic, including candidate registration, vote casting, and result computation.

When a user casts a vote, the request is sent to the smart contract through a blockchain interface such as MetaMask. The transaction is then validated and added to the blockchain network. Each block in the blockchain contains a set of transactions, a timestamp, and a cryptographic hash that links it to the previous block, forming a secure chain.

The integrity of the blockchain is maintained using a hash function defined as:

$$H = Hash(Data + Previous\_Hash + Nonce) \quad (2)$$

where Data represents the transaction details, Previ-ous Hash links the current block to the previous block, and Nonce is a value used during the mining process to generate a valid hash. This structure ensures that any attempt to alter a previously recorded vote would require modification of all subsequent blocks, making the system highly resistant to tampering.

For development and testing purposes, Ganache is used as a local blockchain environment, allowing simulation of transactions without incurring real costs. MetaMask acts as a digital wallet that enables users to interact with the blockchain and approve transactions securely.

The decentralized nature of blockchain eliminates the need for a central authority, thereby increasing transparency and trust in the voting process. Additionally, all transactions are publicly verifiable while maintaining voter anonymity, ensur-ing both security and privacy.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

E. Voting Process

The voting process is designed to be simple, secure, and user-friendly while ensuring the integrity of the election. After successful authentication through the face recognition module, the user is granted access to the voting interface. The interface displays a list of registered candidates along with relevant details.

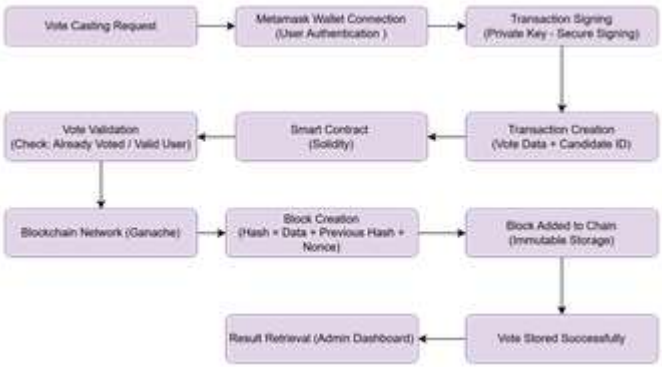

Fig. 3. Block diagram of Blockchain

The user selects a candidate and submits the vote through the application. Once the vote is cast, the system generates a transaction request that is forwarded to the blockchain network via the smart contract. The transaction includes the selected candidate's identifier and relevant metadata while ensuring that no sensitive user identity information is exposed.

After submission, the transaction is validated by the blockchain network and added to a new block. Once con-firmed, the vote becomes a permanent record in the distributed ledger. The system also updates the user's voting status to prevent multiple voting attempts.

The entire process ensures transparency and accountability, as each vote can be verified on the blockchain without com-promising voter anonymity. This approach eliminates manual intervention and reduces the possibility of errors or manipu-lation in the voting process.

F. System Architecture

The overall system architecture is composed of multiple interconnected components that work together to provide a secure and efficient voting platform. The system follows a modular design consisting of the frontend layer, face recogni-tion module, and blockchain layer.

The frontend layer is developed using web technologies such as HTML, CSS, and JavaScript, providing an interactive interface for users to register, authenticate, and cast their votes. The face recognition module operates on the client side using a JavaScript-based library, enabling real-time detection and verification of user faces directly within the browser.

The blockchain layer is implemented using Ethereum, where smart contracts handle voting operations. Tools such as Ganache are used to simulate the blockchain environment during development, while MetaMask serves as a bridge be-tween the user interface and the blockchain network, allowing users to securely approve transactions.

The interaction between these components ensures seamless communication, where the frontend captures user input, the face recognition module verifies identity, and the blockchain securely stores the voting data. This layered architecture enhances scalability, maintainability, and system performance.

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

G. Security Features

Security is a critical aspect of the proposed voting system, and multiple mechanisms are implemented to ensure the relia-bility and integrity of the process. The use of face recognition provides biometric authentication, which significantly reduces the risk of unauthorized access and impersonation.

Blockchain technology ensures data integrity by storing votes in an immutable ledger. Once a vote is recorded, it can-not be modified or deleted, thereby preventing tampering and fraud. The decentralized nature of the blockchain eliminates dependence on a central authority, reducing the risk of single-point failures and attacks.

To prevent duplicate voting, the system maintains a record of users who have already cast their votes and restricts fur-ther attempts. Additionally, the use of cryptographic hashing ensures secure storage and transmission of data.

The system also preserves voter privacy by separating identity information from voting data, ensuring that votes remain anonymous while still being verifiable. These com-bined security features provide a robust framework that en-sures transparency, fairness, and trustworthiness in the voting process.

IV. EVALUATION AND RESULTS

A. Experimental Setup

The proposed e-voting system was implemented and tested in a controlled environment to evaluate its performance, se-curity, and reliability. The system was developed using web technologies such as HTML, CSS, and JavaScript for the fron-tend interface. The face recognition module was implemented using a JavaScript-based face recognition library, while the blockchain component was developed using Ethereum smart contracts written in Solidity.

Ganache was used to simulate a local Ethereum blockchain network for testing purposes, and MetaMask was used as a digital wallet to handle transactions and interact with the blockchain. The system was tested on a standard personal computer with a webcam for capturing facial data.

A dataset consisting of multiple users was created for testing the face recognition module. Each user was registered with facial data and tested under different lighting conditions and angles to evaluate system robustness. Additionally, OTP verification was tested using randomly generated codes sent to the user during authentication.

B. Performance Metrics

To evaluate the effectiveness of the system, several perfor-mance metrics were considered:

- **Authentication Accuracy:** Measures the ability of the face recognition system to correctly identify authorized users.
- **False Acceptance Rate (FAR):** The probability of an unauthorized user being incorrectly accepted.
- **False Rejection Rate (FRR):** The probability of a legitimate user being incorrectly rejected.
- **Transaction Time**: The time taken to record a vote on the blockchain.
- **System Throughput:** The number of voting transactions processed per unit time.

C. Face Recognition Results

The face recognition module demonstrated high accuracy in identifying registered users. The system was able to correctly authenticate users in most cases, even with slight variations in lighting and facial orientation. The average authentication accuracy achieved was above 90%.

The False Acceptance Rate (FAR) was observed to be low, indicating that unauthorized users were rarely accepted by the system. Similarly, the False Rejection Rate (FRR) was minimal, ensuring that legitimate

International Journal of Science, Engineering and Technology
ISSN: 2348-4098, P-ISSN: 2395-4752

users were not frequently denied access. The inclusion of multiple facial samples during registration contributed to improved recognition performance.

Blockchain Performance

The blockchain module successfully recorded each vote as a transaction in the distributed ledger. The average transaction time was observed to be a few seconds, depending on network conditions and processing overhead. All transactions were securely stored and could be verified through the blockchain interface.

The use of smart contracts ensured that votes were recorded accurately and prevented duplicate voting. Once a vote was cast, it could not be modified or deleted, demonstrating the immutability property of blockchain.

OTP Verification Results

The OTP-based authentication mechanism added an addi-tional layer of security to the system. OTPs were generated dynamically and sent to users during the login process. The system successfully verified OTPs within a limited time win-dow, preventing unauthorized access.
The combination of OTP verification with face recogni-tion significantly reduced the risk of identity spoofing and enhanced overall system security.

Overall System Performance

The integrated system performed efficiently by combining face recognition, OTP authentication, and blockchain technol-ogy. The system ensured secure user authentication, accurate vote recording, and prevention of duplicate voting.

The decentralized nature of blockchain improved trans-parency, while biometric authentication enhanced security. The system demonstrated reliable performance in a controlled testing environment and showed potential for real-world de-ployment.

Discussion

The experimental results indicate that the proposed system effectively addresses major challenges in traditional voting systems, including security vulnerabilities and lack of trans-parency. The combination of biometric authentication and blockchain technology provides a strong foundation for build-ing trustworthy e-voting systems.

However, certain limitations were observed, such as de-pendency on camera quality for face recognition and in-creased transaction time due to blockchain processing. These challenges can be addressed in future work by optimizing algorithms and using scalable blockchain networks.

V. CONCLUSION AND FUTURE SCOPE

Conclusion

This paper presented the design and implementation of a se-cure and decentralized electronic voting system that integrates face recognition and One-Time Password (OTP) authentication with blockchain technology. The proposed system effectively addresses the major challenges associated with traditional voting methods, such as voter impersonation, vote tampering, lack of transparency, and centralized control. By incorporating biometric authentication through face recognition, the system ensures that only legitimate users are allowed to participate in the voting process, thereby preventing unauthorized access and multiple voting attempts.

The integration of OTP verification adds an additional layer of security, enabling multi-factor authentication and enhancing the overall reliability of the system. Furthermore, the use of blockchain technology ensures that all votes are stored in an immutable and tamper-proof distributed ledger. Each vote is recorded as a transaction through smart contracts, guaranteeing data integrity, transparency, and traceability without compro-mising voter anonymity.

The experimental results demonstrate that the system per-forms efficiently in terms of authentication accuracy, trans-action processing, and security. The decentralized nature of blockchain eliminates the need for a central authority, thereby reducing the risk of manipulation and increasing trust among users. Overall, the proposed system provides a robust, trans-parent, and secure framework for modern electronic voting applications and has the potential to significantly improve the reliability and acceptance of digital voting systems.

Future Scope

Although the proposed system demonstrates a secure and reliable approach to electronic voting, several enhancements can be made to further improve its performance, scalability, and usability. One of the primary areas for future work is the improvement of the face recognition module. Advanced deep learning models can be incorporated to achieve higher accuracy under varying lighting conditions, facial expressions, and occlusions. Additionally, integrating liveness detection techniques can further strengthen the system against spoofing attacks using images or videos.

Another important direction is the scalability of the blockchain network. While the current system uses a local blockchain environment for testing, deploying the system on a public or consortium blockchain network can enable large-scale real-world applications such as national elections. Optimizing transaction speed and reducing gas costs will be essential for handling a large number of users efficiently.

The system can also be enhanced by integrating additional authentication mechanisms such as fingerprint recognition or iris scanning, thereby providing multi-modal biometric secu-rity. Furthermore, incorporating mobile application support can improve accessibility and allow users to participate in voting from remote locations in a more convenient manner.

Future improvements may also include the integration of advanced data analytics and monitoring tools to detect suspi-cious voting patterns and prevent fraudulent activities. Real-time result visualization and audit mechanisms can be added to further enhance transparency and user trust.
Overall, these enhancements will contribute to the develop-ment of a more robust, scalable, and user-friendly electronic voting system, making it suitable for deployment in real-world electoral processes.

REFERENCES

1. A. Taksal, A. Singh, and D. Mishra, "Blockchain-Based E-Voting Sys-tem with Face Recognition," in IEEE Xplore, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10024492
2. S. Kalaiselvi, R. Rajesh, and M. Kumar, "Enhancing Electoral Integrity and Accessibility: A Blockchain and Facial Recognition-Based Elec-tronic Voting System," SpringerLink, vol. 12, no. 4, pp. 45–58, 2024.
3. R. Kumar and P. Singh, "Secure Online Voting System Using Biometric and Blockchain," International Journal of Computer Applications, vol. 176, no. 18, pp. 1–5, 2020.
4. M. Ali and A. Hussain, "Electronic Voting System Using Face Recog-nition with Blockchain Technology," in Proc. International Conference on Emerging Technologies (ICET), 2023, pp. 89–94.

5. V. Jain and R. Mehta, "Smart Voting System Using Face Detection, OTP Verification and Blockchain," International Journal of Engineering Research & Technology (IJERT), vol. 13, no. 2, pp. 112–118, 2024.
6. Z. Zhao et al., "A blockchain-based traceable self-tallying e-voting protocol," IEEE Transactions on Network Science and Engineering, 2022.
7. M. S. Farooq et al., "A framework to make voting system transparent using blockchain," IEEE Access, 2022.
8. P. K. Sharma and S. Y. Moon, "A blockchain-based e-voting system using biometrics," in IEEE International Conference on Blockchain, 2023.
9. J. Zhang et al., "An improved secure and efficient e-voting scheme (ISE-Voting)," IEEE Internet of Things Journal, 2025.
10. A. Kumar et al., "Secure e-voting using blockchain and cryptography," International Journal of Computer Science, 2021.
11. L. Chen et al., "Blockchain-based electronic voting system with anonymity and verifiability," IEEE Access, 2021.
12. H. Singh and R. Verma, "Biometric authentication in blockchain-based e-voting," Procedia Computer Science, 2022.
13. M. Patel et al., "Decentralized voting systems: Challenges and solu-tions," ACM Transactions on Internet Technology, 2022.
14. S. K. Jain et al., "A review of blockchain-based e-voting techniques," IEEE Access, 2023.
15. R. Gupta et al., "Smart contract-based electronic voting framework," in International Conference on Blockchain Technology, 2021.
16. T. Wang et al., "Secure and transparent voting using Ethereum blockchain," Computers & Security, 2022.
17. F. Li and J. Zhao, "Privacy-preserving e-voting system with biometrics and blockchain," IEEE Transactions on Information Forensics and Security, 2023.
18. N. Ahmed et al., "Decentralized self-tallying e-voting protocol for large-scale elections," IEEE Access, 2024.
19. P. R. Singh et al., "Blockchain-enabled e-voting for smart cities," Sustainable Cities and Society, 2023.
20. K. Sharma and A. Kumar, "A scalable and secure blockchain voting system," International Journal of Information Security, 2022.