International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 2, 2026

Block Chain Based Voting System

A. Kavya[1],Yasmeen Farha[2],Gazala Mariyam[3], Hafsa Tahseen[4]

[1]Assistant Professor;Department Of Computer Science And Engineering(Ai&Ml) Bhoj Reddy Engineering College For Women Hyderabad India

[2,3,4]B.Tech Students; Department Of Computer Science And Engineering(Ai&Ml) Bhoj Reddy Engineering College For Women Hyderabad India

Mail Id; yasmeenmohammed745@gmail.com[2],gazalamariyam6@gmail.com[3], hafsatahseen02@gmail.com[4]

Abstract

Free and fair elections are fundamental to democratic societies, and maintaining the integrity, security, and transparency of the voting process is critical for public confidence. Conventional voting approaches, including paper ballots and electronic voting machines, often encounter challenges such as vote tampering, lack of transparency, delayed vote counting, and limited audit capabilities. These issues can undermine trust in electoral outcomes.This research proposes a Blockchain-Based Voting System that leverages the decentralized and immutable characteristics of blockchain technology to create a secure and transparent digital voting platform. The proposed system utilizes the Ethereum blockchain to record each vote as a permanent transaction, ensuring that once a vote is submitted it cannot be altered or removed. Smart contracts are employed to enforce election rules, verify voter eligibility, and guarantee the principle of one voter–one vote without relying on a centralized authority.

By integrating cryptographic security, distributed consensus, and decentralized data storage, the system enhances voter authentication, prevents unauthorized modifications, and enables real-time verification of election results. Furthermore, the blockchain ledger provides a transparent and auditable record of the voting process while preserving voter privacy.

Keywords: *Blockchain Voting, Ethereum, Smart Contracts, Secure Elections, Digital Democracy, Decentralized Systems, E-Voting Security*

Introduction

The Blockchain-Based Voting System is designed as a secure and transparent digital platform intended to improve the reliability and efficiency of the electoral process through decentralized technologies. The system utilizes blockchain infrastructure to record voting transactions in a distributed ledger where each vote is permanently stored and protected from unauthorized modification. By leveraging blockchain properties such as immutability, transparency, and decentralization, the platform ensures that every voting transaction is securely verified and maintained across multiple nodes within the network.The proposed system operates through a web-based interface that connects users to blockchain services responsible for vote storage and verification. This platform enables voters to participate in elections remotely while maintaining strong security measures and transparency throughout the voting lifecycle. The decentralized nature of the blockchain removes dependence on centralized authorities, thereby reducing risks related to data manipulation or system compromise.In addition to improving transparency, the proposed platform reduces the probability of manual errors and prevents duplicate voting attempts. Security is maintained through cryptographic hashing techniques and distributed validation mechanisms that protect the integrity of stored records. The system is designed to support scalability, enabling its use in various environments ranging from institutional elections to national voting scenarios. Furthermore, the architecture provides opportunities for future enhancements such as mobile-based voting applications, multi-tier election management, and advanced authentication mechanisms.

Existing System

Conventional voting systems commonly rely on paper ballots or basic electronic voting machines, both of which present several operational and security challenges. In traditional voting processes, votes are typically cast manually and subsequently verified through manual counting procedures. These processes can be time-consuming and are often susceptible to errors during vote tabulation and verification.Another limitation of existing voting systems is the reliance on physical identification documents for voter authentication. This approach increases the likelihood of identity misuse and fraudulent voting practices. Additionally, voting data is frequently stored in isolated systems or physical records, which limits transparency and makes it difficult to verify the authenticity of election results. The absence of an integrated digital infrastructure further complicates efforts to ensure accountability and traceability in election management.

Proposed System

The proposed Blockchain-Based Voting System introduces a secure and automated digital voting environment built upon blockchain technology and web-based interfaces. The system integrates essential election activities—including voter registration, identity verification, vote casting, and result recording—into a unified and tamper-resistant

framework. Election administrators can manage candidate information, maintain voter records, and monitor election progress, while blockchain technology ensures that each recorded vote remains immutable and verifiable.The combination of cryptographic hashing, decentralized storage, and smart contract validation provides a robust security framework for the voting process. These mechanisms prevent duplicate voting attempts, restrict unauthorized access, and ensure the integrity of recorded election data. Through its transparent and scalable architecture, the system enhances trust in digital elections while ensuring efficient vote processing and accurate result generation.

Literature Survey

Research in the domain of electronic voting systems has significantly expanded over the past decade due to growing concerns regarding the security and transparency of traditional voting methods. Early studies highlighted that paper-based ballots and basic electronic voting machines are susceptible to manipulation, identity misuse, and limited verifiability. Many researchers have pointed out that centralized voting infrastructures often lack strong auditing capabilities and remain vulnerable to data tampering or system failure. These shortcomings have motivated researchers to investigate advanced technological solutions capable of strengthening election security and reliability.Biometric authentication has emerged as one such approach to improve voter verification processes. Several studies demonstrate that biometric techniques, including fingerprint recognition and facial identification, can effectively prevent impersonation and duplicate voting. For example, research conducted by BalaMurali and colleagues proposed a biometric-based voting machine that ensures only authenticated individuals are permitted to participate in elections. Similarly, Pomares and co-researchers explored the use of facial recognition technologies to enhance voter identification and reduce identity fraud. Although these approaches improve authentication accuracy, concerns regarding biometric data protection and system deployment costs remain important considerations.Another line of research focuses on integrating Internet of Things (IoT) technologies into voting systems to improve accessibility and monitoring capabilities. IoT-based voting platforms allow election authorities to monitor voting activities in real time and facilitate remote participation. Arun and collaborators developed an IoT-enabled voting system using Arduino technology that improves efficiency in vote collection and monitoring. Despite these advantages, IoT-based systems introduce potential security risks related to network vulnerabilities and unauthorized data access, particularly in large-scale deployments.The emergence of blockchain technology introduced new possibilities for developing secure and transparent voting platforms. Blockchain systems operate as decentralized ledgers that store information in immutable blocks, ensuring that once data is recorded it cannot be modified without consensus from network participants. Research by Kumar and Singhi emphasized that blockchain-based voting systems provide enhanced transparency, tamper resistance, and elimination of centralized control mechanisms. Jafar and colleagues further examined blockchain voting frameworks and highlighted their ability to provide verifiable and secure vote storage while identifying challenges related to scalability and privacy preservation.More recent research explores the integration of intelligent technologies within blockchain voting environments. Cryptographic voting protocols have also contributed to the evolution of secure electronic voting frameworks. Early research by Kiayias and Yung introduced self-tallying election mechanisms that ensure ballot secrecy while allowing decentralized vote counting. Rivest and Smith later proposed protocols such as ThreeBallot and VAV that improve transparency and voter verifiability without compromising privacy. These foundational approaches laid the groundwork for modern blockchain-based voting systems that integrate cryptographic security with decentralized infrastructures.

Requirement Analysis

Requirement analysis plays a crucial role in defining the operational capabilities and technical specifications of the proposed blockchain-based voting platform. The system requirements are categorized into functional requirements, non-functional requirements, and computational resource requirements to ensure that the platform operates efficiently, securely, and reliably.The functional requirements define the core services provided by the system. The administrative module allows election authorities to manage voter registration, candidate information, and election schedules. Administrators can monitor voting activities, verify voter records, initiate or terminate election sessions, and generate final results based on recorded votes. On the other hand, the voter module enables users to register within the system, authenticate their identity through secure verification methods such as facial recognition and email-based one-time passwords, review candidate details, and cast their vote through a secure interface. After voting, the system provides confirmation that the vote has been successfully recorded on the blockchain ledger.Non-functional requirements describe the quality attributes that ensure the reliability and usability of the system. The platform must provide an intuitive user interface to allow voters and administrators to interact with the system easily. Security mechanisms such as blockchain storage, biometric verification, and OTP

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

authentication are required to protect sensitive data and voting records. The system must remain continuously available during election periods and must maintain reliable performance even when handling large numbers of voters. Scalability is also an essential requirement, enabling the system to accommodate future expansion without compromising performance. Data integrity mechanisms such as cryptographic hashing ensure that stored voting records remain accurate and unaltered.The computational resource requirements include both hardware and software components necessary to support the system's functionality. The hardware infrastructure should include a processor equivalent to Intel Core i5 or higher, at least 8 GB of system memory, a webcam for facial recognition authentication, and sufficient storage capacity to maintain system data. The software environment includes operating systems such as Windows, Linux, or macOS, along with programming languages including Python and JavaScript for system development. Frameworks such as Node.js and development tools like Visual Studio Community Edition are used for implementation, while blockchain technology functions as the primary data storage mechanism for vote transactions. Additional libraries and application programming interfaces—including OpenCV, Web3.js, and machine learning frameworks such as TensorFlow or Keras—support facial recognition and blockchain interaction within the system.To guide the development process, the project adopts an iterative life cycle model. In the first phase, system requirements are analyzed and system actors such as voters and administrators are identified. The second phase focuses on system design and implementation, including the development of modules for voter registration, authentication, and blockchain-based vote recording. Smart contracts are implemented to automate election processes and ensure secure vote validation. The final phase involves comprehensive system testing and deployment, where authentication accuracy, vote transactions, and blockchain operations are verified to ensure system reliability. Each development iteration enhances the platform's security, transparency, and operational efficiency, ultimately resulting in a robust blockchain-based digital voting system.

System Design

System Architecture

System design describes the structural organization of components involved in the development of the proposed blockchain-based voting platform and explains how requests are processed throughout the system. In software engineering, architecture represents a structured description of system components and their relationships, enabling developers to understand the system's organization and functionality. A well-defined architecture allows developers to analyze system performance, maintain scalability, and ensure efficient communication between modules.The architecture of the proposed voting system is divided into three primary layers: the frontend layer, the backend layer, and the blockchain layer. The frontend layer acts as the user interface through which voters and administrators interact with the system. It provides functionalities such as user registration, authentication, candidate viewing, and vote submission. This interface is designed to be simple and intuitive so that users can easily participate in the election process without requiring advanced technical knowledge.

The backend layer performs the core application logic and handles tasks such as user authentication, request validation, and communication with the blockchain network. It processes user inputs, verifies voter eligibility, manages candidate information, and ensures that only authorized actions are executed within the system. Additionally, the backend layer manages communication between the frontend interface and the blockchain network.The blockchain layer represents the decentralized infrastructure responsible for secure storage and verification of voting transactions. Each vote submitted by a user is recorded as a blockchain transaction, which is then validated and permanently stored in a distributed ledger. This decentralized approach ensures that vote records remain transparent, immutable, and resistant to unauthorized modifications.

Software Architecture

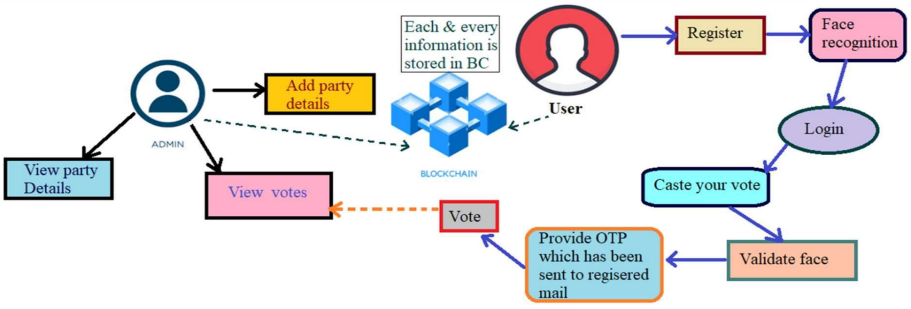

Fig. 1 SOFTWARE ARCHITECTURE

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

The software architecture illustrates how different software components of the system interact with one another to perform voting operations. It demonstrates the relationship between the user interface, backend services, authentication modules, and blockchain services. The architecture ensures that user requests are processed efficiently while maintaining system security and reliability.

Within this structure, the frontend interface communicates with backend APIs that handle authentication, vote processing, and data management. The backend server then interacts with blockchain nodes through specialized libraries such as Web3.js to store and retrieve vote transactions. This layered architecture ensures modularity, making it easier to maintain and upgrade the system.

Technical Architecture

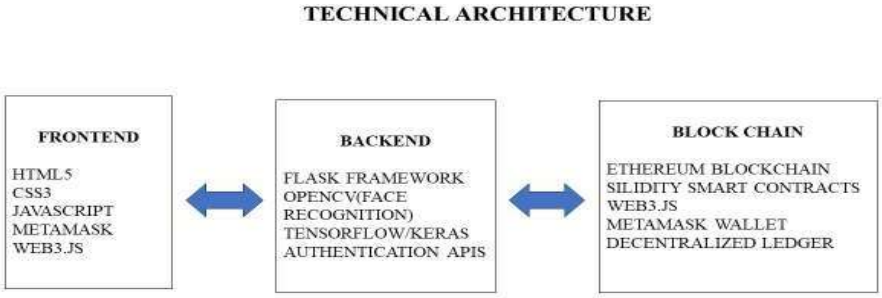

Fig 2 TECHNICAL ARCHITECTURE

The technical architecture focuses on the technologies and tools used to implement the proposed system. It highlights the integration of web technologies, machine learning libraries, and blockchain frameworks that collectively enable secure digital voting. The frontend interface is implemented using web development technologies that allow users to interact with the system through a browser. The backend server processes requests and manages application logic, while blockchain technology ensures decentralized and tamper-proof storage of votes.

Sequence Diagram

Component Diagram

A component diagram provides a high-level view of system components and their dependencies. It identifies the major modules within the application and illustrates how they interact with each other. In the proposed system, the main components include the user interface, backend server, authentication modules, and blockchain network.

The user interface allows voters and administrators to interact with the platform. The backend server manages application logic and processes requests received from the frontend interface. Authentication modules handle identity verification processes including biometric validation and OTP confirmation. The blockchain network stores vote transactions in a decentralized ledger, ensuring transparency and immutability of voting records. The component diagram demonstrates how these modules collectively enable secure and efficient digital voting.

Implementation

Technologies Used

The implementation of the proposed blockchain-based voting system integrates modern web technologies, blockchain frameworks, and biometric authentication techniques to ensure secure vote casting and storage. The system development begins with the configuration of the development environment, where tools such as Node.js, Python, Ethereum, MetaMask, and Web3.js are installed. These tools enable backend processing, blockchain interaction, and integration with decentralized networks.During the voter registration stage, user details and biometric data are collected through web-based forms. Facial images are captured using camera devices and processed through computer vision libraries such as OpenCV. Once validated, the vote is permanently stored in the blockchain ledger, ensuring transparency and immutability.

Pseudocode Description

The voting system operates through several key functional procedures including voter registration, authentication, vote casting, blockchain storage, and result generation. During the registration phase, voter details and facial images are captured and stored within the system database. If a voter's information already exists in the database, the system prevents duplicate registration.Authentication is performed by capturing a live facial image and comparing it with the stored dataset. If the system identifies a match, the voter is granted access to the voting interface. Once authenticated, the voter is allowed to select a candidate and submit the vote. The system verifies whether the voter has previously participated in the election before processing the transaction.

Testing

Software testing plays an essential role in verifying the functionality, reliability, and security of the blockchain-based voting system. Since voting applications require high levels of trust and accuracy, thorough testing is necessary to ensure that the system operates correctly under various conditions. Even minor errors in the voting process may lead to incorrect results or security

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

vulnerabilities, making testing a critical stage of the development process.Testing helps identify defects, validate system requirements, and ensure that all components function as intended. It also improves user confidence by verifying that the system securely processes votes and prevents unauthorized access. Through systematic testing procedures, the reliability and transparency of the voting platform can be significantly enhanced.

Testing Dimensions

Several testing dimensions were considered to ensure the quality and performance of the proposed system. The application layers—including frontend interfaces, backend services, and blockchain infrastructure—were tested to confirm smooth interaction between system components. Testing was conducted at multiple levels including unit testing, integration testing, and system testing to validate both individual modules and the entire application.

Different testing approaches such as functional testing, performance evaluation, security testing, and usability assessment were also applied. Functional testing ensured that features such as voter registration and vote casting operated correctly, while performance testing evaluated the system's response time and scalability. Security testing focused on verifying authentication mechanisms and preventing unauthorized access. Additionally, data validation procedures were implemented to ensure that vote transactions remained accurate and tamper-proof.

Testing Stages

Testing of the blockchain-based voting system was conducted in several stages. Unit testing was first performed to evaluate individual components such as voter registration, facial authentication, OTP verification, and vote submission modules. Each component was tested independently to confirm that it produced correct outputs for valid inputs.Integration testing was then carried out to verify the interaction between different modules including frontend interfaces, backend services, and blockchain transactions. This stage ensured that data was transferred correctly across system components without errors.System testing involved evaluating the complete voting workflow, including voter registration, authentication, vote casting, and result generation. The purpose of this stage was to confirm that the system met all functional and performance requirements.

Result

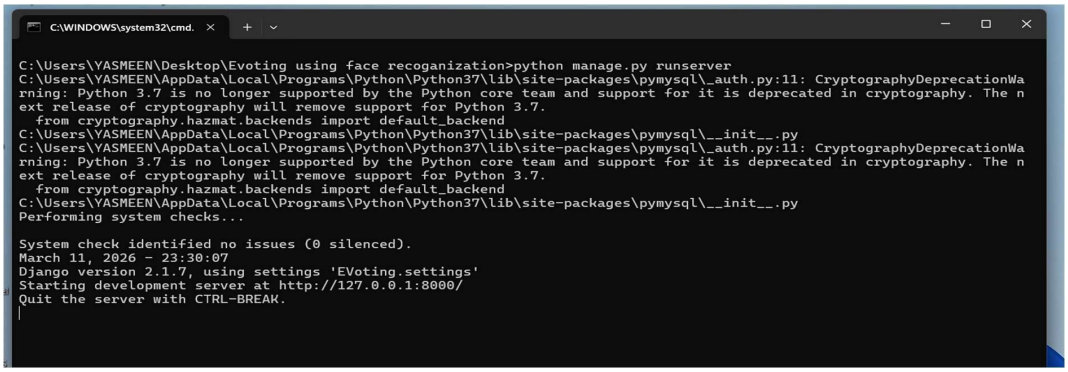

Fig 3 : ACTIVATE PROJECT

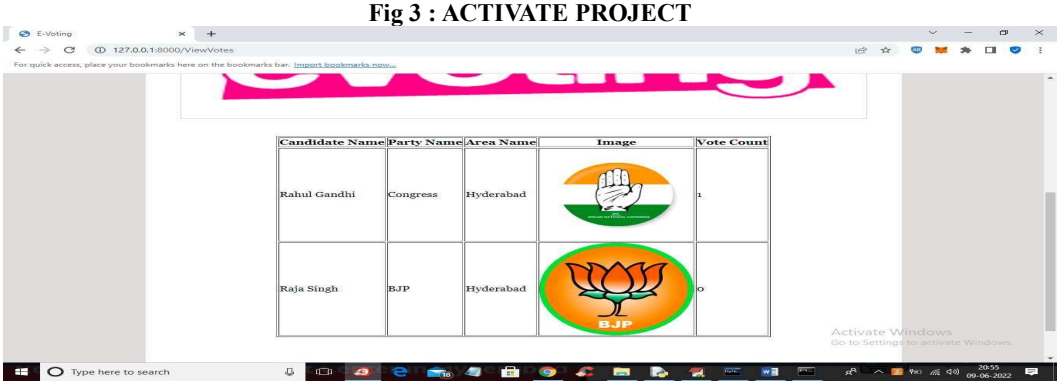

Fig 4: ADMIN OUTPUT

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 2, 2026

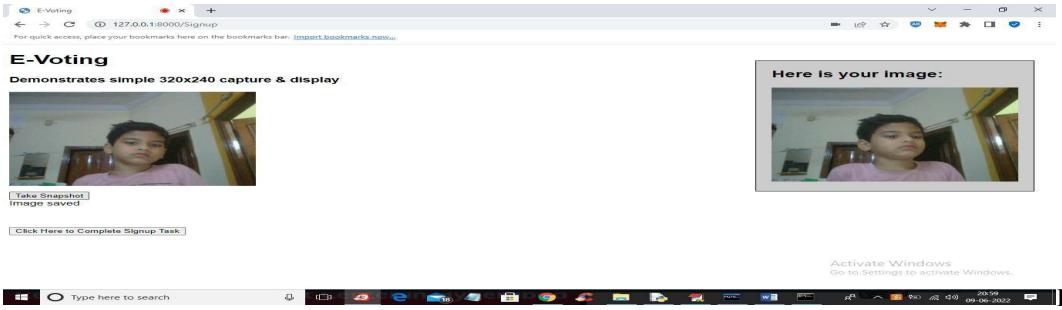

Fig 7.: 5 USER OUTPUT

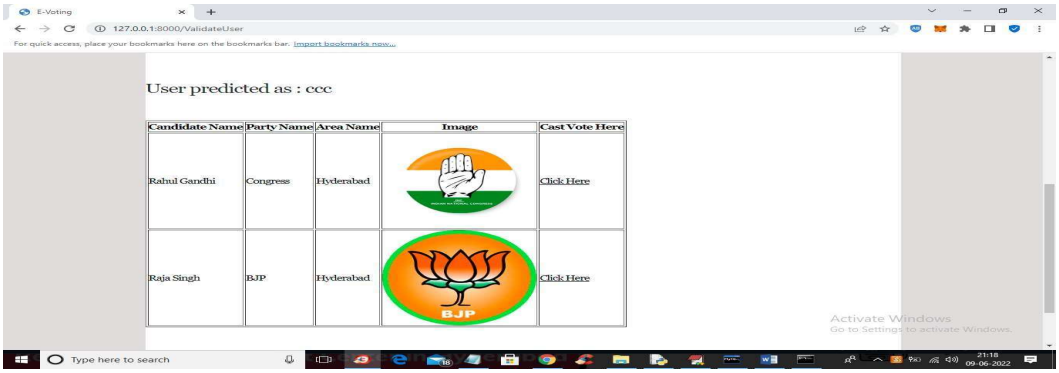

Fig 6 USER OUTPUT

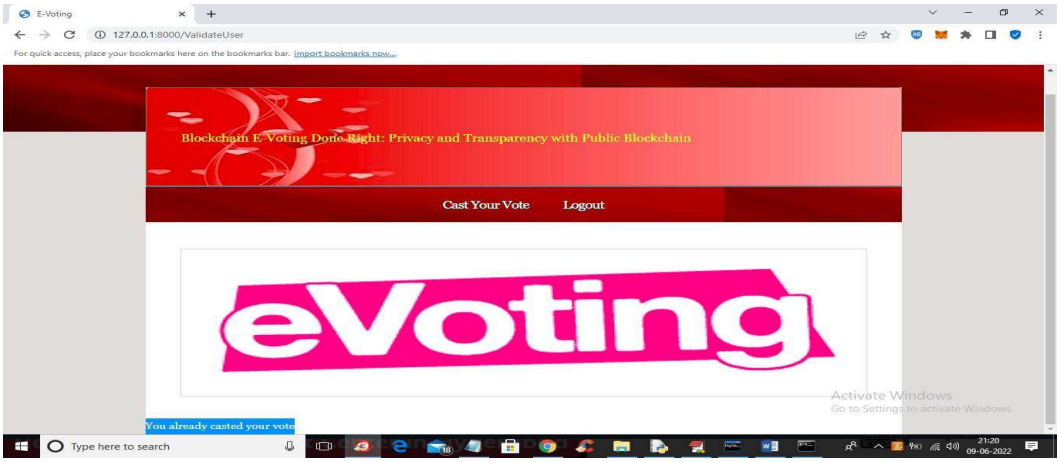

Fig 7 USER OUTPUT

Conclusion

The proposed Blockchain-Based Voting System effectively demonstrates how modern digital technologies can enhance the reliability, transparency, and security of electoral processes. By integrating blockchain infrastructure with biometric authentication mechanisms such as facial recognition and one-time password (OTP) verification, the system ensures that only authorized individuals are allowed to participate in the voting process. This multi-layered authentication approach significantly reduces the risk of identity fraud and unauthorized access.A key feature of the system is the use of blockchain technology to store votes as immutable transactions. Once a vote is recorded on the blockchain ledger, it cannot be modified or deleted, ensuring the integrity and transparency of the election data. This decentralized storage approach eliminates the risk of centralized data manipulation and strengthens trust in the election process. Furthermore, the system prevents duplicate voting attempts by validating voter identity and tracking participation records through secure mechanisms.The implementation also simplifies election management by automating key processes such as voter verification, vote recording, and result generation. The platform provides an intuitive user interface that allows both administrators and voters

to interact with the system efficiently. Additionally, cryptographic hashing and distributed ledger technology ensure that sensitive information remains protected against tampering or unauthorized modifications.

Future Scope

Although the proposed blockchain-based voting platform provides a secure and transparent voting framework, several improvements can be explored in future research to enhance system capabilities and scalability.One potential improvement involves the integration of advanced biometric authentication techniques such as fingerprint recognition, iris scanning, or multi-factor authentication methods. Incorporating multiple authentication layers can further strengthen identity verification and improve the overall security of the voting system.Another promising extension is the development of mobile-based voting applications. By enabling secure voting through smartphones or mobile devices, the system can increase accessibility and encourage greater participation, particularly for voters who are unable to visit physical polling stations.Future research can also focus on integrating the voting platform with government identity verification systems, such as national identity databases or digital identity frameworks. Such integration would improve the accuracy of voter authentication and reduce the risk of fraudulent registrations.Scalability is another important aspect for future development. As national elections involve millions of voters, the system can be enhanced by adopting more efficient blockchain infrastructures and consensus algorithms capable of handling large volumes of transactions with minimal latency.

References

[1] P. BalaMurali, P. Sarada Sravanthi, and B. Rupa, "Smart and Secure Voting Machine using Biometrics," *Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC)*, 2020.

[2] K. C. Arun, S. Ahmad, S. Noor, I. Mumtaz, and M. Ali, "Arduino-Based Secure Electronic Voting System with IoT," *4th Global Conference on Computing & Media Technology*, 2020.

[3] S. Kumar and N. Singhi, "A Survey on Smart Electronic Voting System Using Blockchain Technology," *Journal of Emerging Technologies and Innovative Research (JETIR)*, 2020.

[4] M. Pomares, I. Levin, R. M. Alvarez, G. L. Mirau, and T. Ovejero, "Smart E-Voting System with Face Recognition Based on Blockchain Technology," *International Journal of Advanced Research in Computer and Communication Engineering*, 2020.

[5] M. Pawlak, A. Poniszewska-Maranda, and N. Kryvinska, "Towards Intelligent Agents for Blockchain-Based E-Voting Systems," *3rd International Conference on Communication and Electronics Systems (ICCES)*, 2018.

[6] U. Jafar, M. ul Hassan, R. Iqbal, and M. I. Khan, "Blockchain for Electronic Voting Systems: Review and Open Research Challenges," *Sensors*, 2021.

[7] A. Kiayias and M. Yung, "Self-Tallying Elections and Perfect Ballot Secrecy," *Public Key Cryptography Conference*, 2002.

[8] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[9] R. Rivest and W. Smith, "Three Voting Protocols: ThreeBallot, VAV, and Twin," *USENIX/ACCURATE Electronic Voting Technology Workshop*, 2007.

[10] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*, Pearson Education, 2018.

[11] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," 2014.

[12] Linux Foundation, "Hyperledger Fabric Documentation," 2020.

[13] A. Singh and K. Chatterjee, "Cloud-Based Secure Voting System Using Blockchain Technology," *International Journal of Computer Science and Information Security*, 2019.

[14] S. K. Sharma and R. Gupta, "Secure Online Voting System Using Blockchain and Biometrics," *International Journal of Engineering Research & Technology (IJERT)*, 2020.

[15] P. Tarasov and H. Tewari, "The Future of E-Voting: Blockchain and Internet Voting," *IEEE Security & Privacy*, 2017.