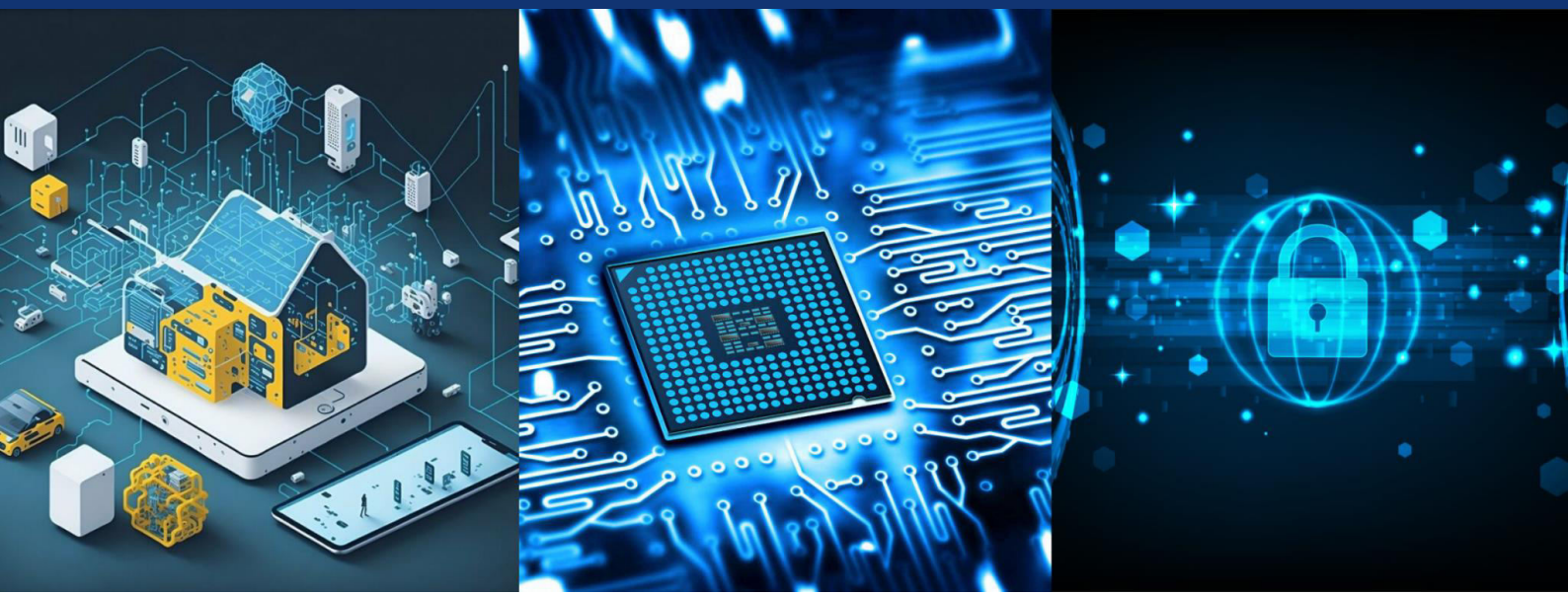
IJIRCCE

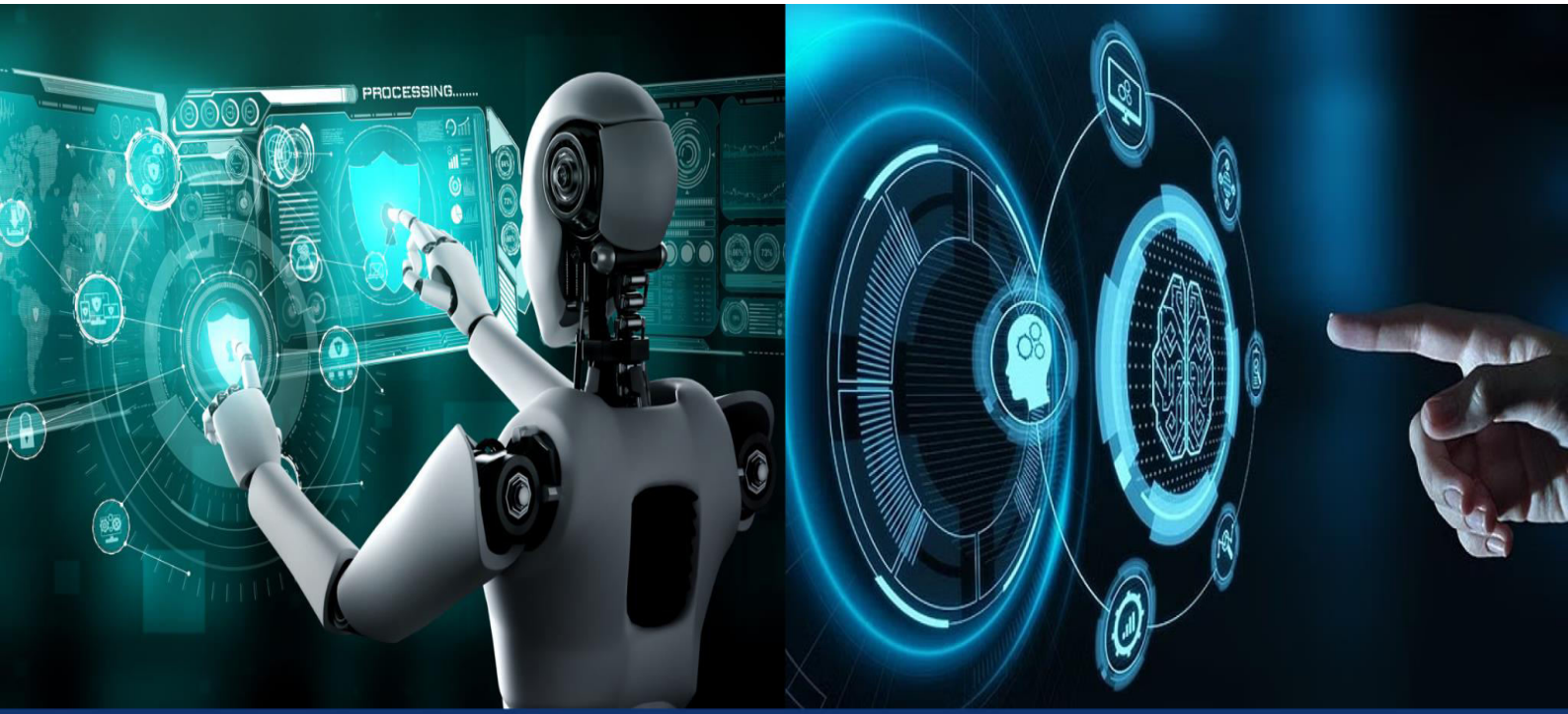
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 13, Issue 3, March 2025

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303084

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Blockchain based Voting using Biometric Authentication

Dr. Manjusha Deshmukh, Harshada Ramole, Prathmesh Kode, Jisha Shaji, Shreeya Zemse

Associate Professor, Dept. of CS (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CS (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CS (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CS (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

UG Student, Dept. of CS (IoT CS BC), A. C. Patil College of Engineering, Navi Mumbai, Maharashtra, India

ABSTRACT: Elections play a crucial role in decision-making processes, where transparency, security, and accessibility are of paramount importance. Traditional voting systems often face challenges such as identity fraud, lack of trust, and inefficiencies in voter authentication. To address these issues, this project introduces a blockchain-based biometric voting system designed exclusively for institutional-level elections. The system leverages blockchain technology to ensure transparency, immutability, and security while integrating biometric authentication for fool proof voter verification. By using fingerprint recognition, the system eliminates the risks of multiple voting, unauthorized access, and identity fraud. Smart contracts automate the voting process, ensuring votes are recorded accurately and cannot be altered or tampered with. The decentralized nature of the blockchain further enhances security by preventing any single entity from manipulating the results. This project also focuses on user-friendly accessibility, enabling institutions to conduct elections efficiently while maintaining voter anonymity and trust. Future enhancements include integrating advanced biometric modalities, real-time vote tracking, and expanding the system's scalability for broader applications. Through blockchain and biometric authentication, this system establishes a secure, transparent, and reliable voting mechanism, paving the way for trust-driven institutional elections.

KEYWORDS: Blockchain, Biometric Authentication, E-Voting, Security, Transparency

I. INTRODUCTION

Ensuring a secure and trustworthy voting process is essential to maintain the integrity of elections. Traditional voting systems often suffer from issues such as identity fraud, unauthorized access, and result manipulation, leading to concerns over transparency and reliability. With advancements in technology, there is a growing need to adopt innovative solutions that enhance security while maintaining ease of use. This project introduces a blockchain-based biometric voting system that leverages modern technologies to provide a fraud-resistant, transparent, and efficient voting mechanism. The system integrates fingerprint authentication to prevent unauthorized voting and identity duplication, ensuring that each voter is uniquely verified. By utilizing blockchain technology, the platform ensures tamper-proof record-keeping, allowing votes to be securely stored in an immutable and decentralized ledger.To further enhance the voting experience, the system incorporates smart contracts for automated vote processing, eliminating manual errors and ensuring trust in the results. Additional features include real-time vote tracking, decentralized storage, and cryptographic security, which collectively strengthen the overall reliability of the system. By combining biometric authentication and blockchain, this project addresses the fundamental weaknesses of conventional voting systems, paving the way for a more secure, transparent, and accessible electoral process.

1.1 OBJECTIVES

To balance security and decentralization in the voting process. To ensure tamper-proof and fraud-resistant elections using blockchain technology. To promote trust and transparency in vote recording and result declaration. To enhance voter authentication through biometric verification. To provide real-time vote tracking and secure storage of voting data. To align with the principles of fair and accessible elections, ensuring every eligible voter has a voice. To eliminate multiple voting and identity fraud through unique biometric authentication. To foster technological innovation in electronic voting systems. To support scalability and adaptability for future election requirements.

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303084

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1.2 PURPOSE

Traditional voting systems often operate in centralized, isolated environments, making them vulnerable to security breaches, fraud, and lack of transparency. The purpose of this project is to introduce a blockchain-based biometric voting system that ensures a secure, transparent, and verifiable election process.

The voting process consists of four key stages:

- Voter Authentication – Ensuring that only eligible voters participate by using biometric verification (fingerprint authentication).
- Vote Casting – Providing a tamper-proof mechanism where each vote is securely stored on a decentralized blockchain ledger.
- Vote Validation – Using smart contracts to automate and verify the voting process, eliminating manual errors and unauthorized modifications.
- Result Declaration – Enabling real-time vote tallying while maintaining anonymity and transparency, ensuring that election outcomes are trustworthy and immutable.

This system aims to enhance security, prevent electoral fraud, and build trust in the voting process by leveraging blockchain's decentralized and transparent nature. Additionally, it aligns with global best practices for secure digital voting and fosters innovation in electoral technology, ensuring a reliable, scalable, and fraud-resistant voting solution.

II. EXISTING SYSTEM

Traditional voting systems, whether paper-based or electronic, have long been the foundation of electoral processes. However, they come with several challenges, including identity fraud, vote manipulation, and lack of transparency. Many countries still rely on electronic voting machines (EVMs), which, despite their efficiency, remain vulnerable to hacking, tampering, and unauthorized access. Additionally, these systems often require manual verification processes, which can introduce human errors and delays in result declaration.

Online voting platforms have also emerged, but they often lack robust security mechanisms, making them susceptible to cyber threats. Furthermore, centralized voting databases create a single point of failure, increasing the risk of data breaches or manipulation. Some existing biometric voting solutions have attempted to address voter authentication issues, but they still face challenges in maintaining data integrity and preventing fraudulent activities.

In contrast, blockchain-based voting has gained attention due to its ability to offer decentralization, security, and transparency. Projects such as Follow My Vote and Voatz have explored blockchain for voting, but concerns regarding scalability, accessibility, and government acceptance remain. Additionally, many blockchain-based voting systems do not incorporate biometric authentication, leaving room for potential vulnerabilities in voter identity verification.

Limitations in Existing Systems or Research Gap

Existing voting systems suffer from multiple security, transparency, and trust issues. Traditional paper-based voting is time-consuming, costly, and prone to manipulation, while electronic and online voting systems face security risks and limited voter verification methods. Centralized databases in online voting platforms also create vulnerabilities that could be exploited.While blockchain technology offers immutability and decentralization, most blockchain-based voting platforms lack biometric authentication, making them vulnerable to identity fraud and unauthorized access. Additionally, many blockchain solutions require complex infrastructures, making implementation challenging. Scalability is another concern, as current blockchain voting solutions struggle with handling large-scale elections efficiently.

Another major research gap is the lack of real-time verification and auditing mechanisms in existing voting systems. Most platforms do not offer instant voter authentication, vote validation, and automatic result tallying, leading to delays and potential tampering. By integrating biometric authentication with blockchain, this project aims to bridge these gaps, ensuring a secure, transparent, and fraud-resistant voting system.

III. PROPOSED SYSTEM

The development of the voting system follows a structured approach to ensure security, transparency, and efficiency. The process begins with problem identification and research, focusing on existing voting systems' challenges and how blockchain and biometric authentication can address them. The next step involves the design and development of core modules, including frontend and backend development, ensuring seamless user interaction. The system integrates biometric authentication for secure voter verification and blockchain technology for transparent, tamper-proof vote

© 2025 IJIRCCE | Volume 13, Issue 3, March 2025| DOI: 10.15680/IJIRCCE.2025.1303084

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

recording. Additional features include smart contracts for automated vote validation, real-time vote tallying, and multi-device accessibility to enhance usability. Security measures such as encryption, multi-factor authentication, and fraud detection are incorporated to safeguard voter data. Following the development phase, the system undergoes rigorous testing and optimization, including unit testing, security audits, and user experience evaluations. A continuous monitoring and feedback loop ensures the system remains secure, scalable, and adaptable to future enhancements

Our decentralized mobile application is designed to address the limitations of traditional institutional voting systems by leveraging blockchain technology, fingerprint authentication, and a secure, transparent, and scalable architecture. The system ensures strong authentication mechanisms through biometric verification, preventing identity fraud and multiple voting attempts. A smart contract-based voting process guarantees transparency and immutability, making the system resistant to tampering. The platform utilizes local MongoDB for efficient data storage and retrieval, while real-time updates enhance the voting experience. Additionally, MetaMask integration enables secure user interaction with the blockchain. Future enhancements include advanced cryptographic techniques for enhanced privacy, AI-driven analytics for voter behaviour insights, and extended Web3 capabilities for seamless decentralization.

3.1 DESIGN DETAILS

The User Interface (UI) of the decentralized voting application consists of a voter dashboard, candidate details page with real-time updates, voting status tracker, user authentication page with fingerprint verification, transaction history for blockchain-based vote logging, and an admin panel for candidate registration and election monitoring. A mobile app interface is planned for future development.

The Real-time Data Module integrates data from multiple sources to ensure secure and transparent voting. Biometric Data is captured using laptop fingerprint sensors and WebAuthn passkeys, providing seamless authentication without external fingerprint devices. Blockchain Data is recorded on an Ethereum smart contract, ensuring immutability and verifiability of votes. Voter Registration Data is securely stored in a local MongoDB database, allowing for efficient retrieval and verification.

The Blockchain Ledger maintains an immutable record of all votes, executes smart contracts for casting and counting votes, and serves as a transparent transaction explorer.

The AI-based Verification System (future work) will enhance security by detecting fraudulent voting attempts, analyzing voting patterns, and preventing multiple registrations.

The MongoDB Database is used for storing voter details, candidate data, and election results. It is designed for scalability to handle institutional-level elections efficiently with real-time updates.

3.2 DESIGN ARCHITECTURE

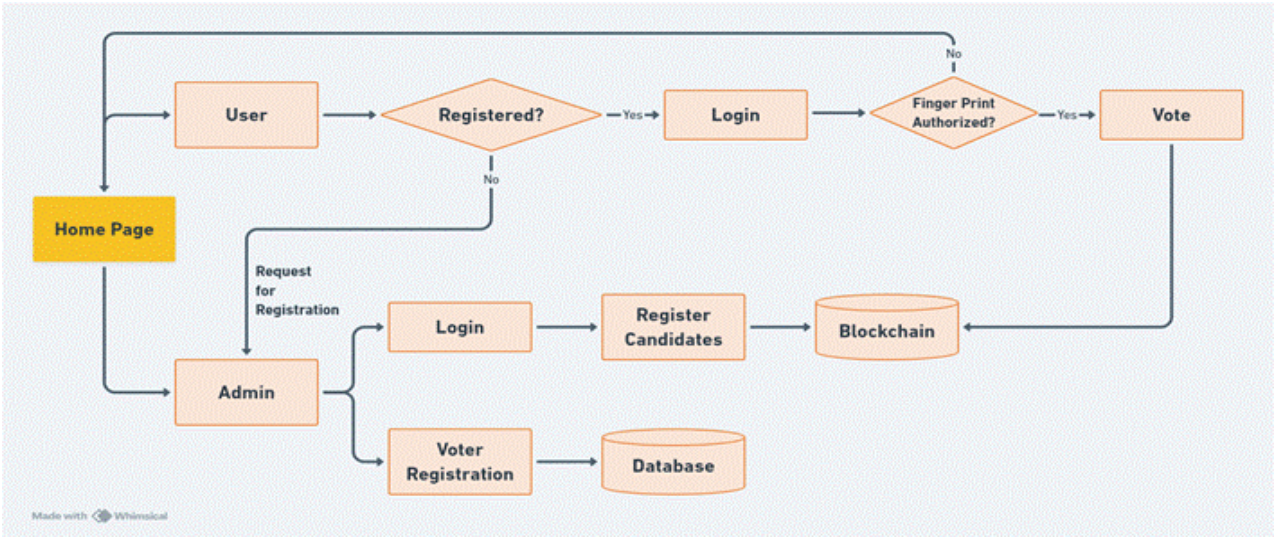


Figure 1: Design Architecture

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. CONCLUSION

Our decentralized fingerprint authentication-based voting system is an innovative approach to institutional-level voting, integrating blockchain transparency, biometric security, and decentralized identity verification. This project aims to eliminate fraud, enhance voter authentication, and ensure a tamper-proof election process, setting a new standard for secure and verifiable online voting.The initial phase of development focused on establishing the system architecture, smart contracts, frontend development, database connectivity, and WebAuthn-based fingerprint authentication (utilizing laptop fingerprint sensors and web passkeys instead of external biometric scanners like MFS100). These foundational components provide a seamless, user-friendly, and highly secure voting experience.Further enhancements will incorporate real-time vote updates, AI-driven fraud detection, advanced candidate filtering, and live election analytics. Blockchain-based smart contracts will securely record votes, ensuring immutability, decentralization, and complete transparency. By leveraging Web 3.0 technologies, decentralized governance, and real-time communication protocols, this system addresses the core challenges of traditional voting methods, such as vote manipulation, identity theft, and centralized control.This project envisions a scalable and future-proof voting mechanism, making institutional elections secure, efficient, and trustable. With its decentralized and biometric-driven approach, it paves the way for modern, tamper-proof, and technology-driven electoral systems.

V. FUTURE SCOPE

The future scope of this decentralized fingerprint authentication-based voting system includes integrating government Aadhaar databases for seamless voter verification, using MFS100 fingerprint sensors alongside laptop fingerprint sensors and Web Passkeys for multi-device authentication. IoT-enabled biometric voting kiosks can further streamline on-site verification, while AI-powered fraud detection will help prevent duplicate votes and ensure election integrity. Smart contracts can be enhanced to automate election rules, dispute resolution, and transparent vote counting. Multi-lingual NLP support will make the system accessible to a diverse population, while decentralized identity management (SSI) will enable secure and reusable voter credentials. Metaverse-based election simulations can educate voters and facilitate candidate debates, while real-time social media integration will boost engagement and transparency. By leveraging Web 3.0 technologies, this system aims to establish a highly secure, tamper-proof, and inclusive voting platform, revolutionizing institutional elections.

REFERENCES

[1] S. S. Hossain et al., "E-voting system using blockchain technology," Proc. 2nd Int. Conf. Blockchain Technol. Appl., 2019.
[2] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7.
[3] F. P. Hjálmarsson et al., "Blockchain-based E-Voting system," Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), 2018.
[4] M. S. Farooq et al., "A framework to make charity collection transparent and auditable using blockchain technology," Comput. Electr. Eng., vol. 83, 2020.
[5] T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," Comput. Netw., vol. 174, 2020.
[6] S. Park et al., "Going from bad to worse: From internet voting to blockchain voting," J. Cybersecurity, vol. 7, no. 1.
[7] K. M. Khan et al., "Secure digital voting system based on blockchain technology," Int. J. Electron. Government Res., vol. 14.
[8] C. K. Adiputra et al., "A proposal of blockchain-based electronic voting system," Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS), 2018.
[9] J. Huang et al., "The application of the blockchain technology in voting systems: A review," ACM Comput. Surv., vol. 54, no. 3.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details