International Journal of
AI Electronics and Nexus Energy
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Real Time Smart Voting System Using Blockchain, Fingerprint And Face Recognition Blockchain

[1]Mandala Anusha,[2]Mrs.G.Swapna
[1]MCA Student, Department Of Master of Computer Applications, Sri Chaitanya Institute Of Technology (Scit) Ponnekal ,Khammam
[1]Email : anushamandala786@gmail.com
[2]Assistant Professor, Department Of Master of Computer Applications, Sri Chaitanya Institute Of Technology (Scit) Ponnekal ,Khammam
[2]Email : swapnabandi1112@gmail.com

ABSTRACT
The Smart Voting System Using Blockchain, Fingerprint, and Face Recognition is a secure and innovative approach to enhance the integrity of voting processes. By leveraging blockchain technology for data storage, fingerprint-based authentication, and facial recognition for identity verification, the system ensures robust security and transparency. The application is divided into two modules: the admin module for managing the voting process and the voter module for securely casting votes. This system provides a seamless and tamper-proof mechanism for conducting elections, ensuring trustworthiness and accessibility.

Keywords: Blockchain, Electronic Voting (E-Voting), Fingerprint Authentication, Face Recognition, Biometric Authentication, Secure Voting System, Voter Verification, Decentralized Ledger, Smart Contracts, Election Security, Identity Authentication, Tamper-Proof Voting, Privacy Preservation, Blockchain-Based Voting, Django Framework.

International Journal of
AI Electronics and Nexus Energy
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

I. INTRODUCTION

Elections are the cornerstone of democracy, ensuring that citizens have the power to choose their representatives. However, traditional voting systems often face challenges related to security, transparency, and voter authentication. Fraudulent practices and data tampering can undermine the credibility of elections, necessitating the development of advanced technologies to address these concerns.

Blockchain technology has emerged as a game-changer in various domains due to its decentralized, secure, and transparent nature. In the context of voting systems, blockchain offers a tamper-proof way to store voter data and election results, ensuring integrity and trust. Biometric verification, including fingerprint and facial recognition, adds an additional layer of security by ensuring that only legitimate voters can participate.

This project presents a Smart Voting System that integrates blockchain technology with biometric and facial recognition to create a highly secure and reliable voting process. The system includes two key modules: the admin module for managing elections and the voter module for participation. The admin module allows administrators to add parties, candidates, and manage voting data. The voter module ensures secure registration and authentication before allowing voters to cast their votes.

A distinguishing feature of this system is its use of blockchain to store registration details, ensuring that the data remains immutable and tamper-proof. Biometric verification is implemented using fingerprint recognition during login, while facial recognition is used before casting a vote. These mechanisms enhance security and eliminate the possibility of identity fraud.

The proposed system addresses the limitations of existing voting processes by providing a robust, transparent, and tamper-resistant solution. This document outlines the key features, advantages, and implementation details of the Smart Voting System Using Blockchain, Fingerprint, and Face Recognition.

II. LITERATURE SURVEY

TITLE: Blockchain-Based E-Voting Systems: A Survey

AUTHORS: Solanki, K., Khandare, M. S. (2020)

ABSTRACT:

The introduction of blockchain technology has revolutionized the concept of voting systems. This paper surveys the use of blockchain for electronic voting systems, focusing on ensuring data integrity, privacy, and tamper-proof voting. Blockchain's decentralized nature allows it to provide transparency and security, which makes it highly suitable for creating a transparent and reliable voting system. The study discusses various blockchain-based e-voting models, their implementations, and challenges faced in terms of scalability, voter anonymity, and technical complexities.

The authors highlight the key advantages of blockchain in e-voting systems, particularly its immutability and decentralized structure. They discuss several blockchain frameworks that could support e-voting systems and emphasize the importance of combining blockchain with other security mechanisms, such as biometric verification and encryption, to ensure the safety and authenticity of votes.

TITLE: Biometric Authentication in Secure Voting Systems

AUTHORS: Kaur, G., Saini, J. R. (2019)

ABSTRACT:

This paper addresses the use of biometric authentication for securing electronic voting systems. The authors propose a secure biometric-based authentication process for the registration and login phases of the voting system. The study reviews the different biometric modalities like fingerprint, face recognition, and iris scans and their

International Journal of
AI Electronics and Nexus Energy
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

effectiveness in terms of voter authentication. The paper concludes that biometric systems, when integrated with e-voting systems, can prevent fraudulent activities such as impersonation and ensure voter identity validation.

The integration of biometric technology enhances security and user experience by eliminating the need for traditional passwords. The study also discusses challenges like the need for high-quality biometric data and how environmental conditions can affect the accuracy of biometric systems in practical scenarios.

TITLE: A Privacy-Preserving Blockchain-Based Voting System

AUTHORS: Zhao, J., Cui, W., Qian, L., Xue, F. (2017)

ABSTRACT:

Blockchain provides an innovative solution to preserve privacy and secure votes in electronic voting systems. This research discusses the privacy-preserving features of blockchain and how it can be applied to voting systems. It explores how blockchain can be used to guarantee voter anonymity while ensuring the integrity and transparency of the voting process. The study presents a privacy-preserving protocol where votes are securely encrypted and stored in the blockchain.

The paper emphasizes the need for privacy protection in digital voting systems and presents a model that balances transparency with voter confidentiality. The proposed model leverages advanced cryptographic techniques, such as zero-knowledge proofs, to ensure that votes are securely recorded without revealing the identity of the voter.

TITLE: Smart Contracts in Blockchain-Based Voting Systems

AUTHORS: Dhanalakshmi, S., Anuradha, J. (2021)

ABSTRACT:

Smart contracts, self-executing contracts with the terms of the agreement directly written into code, can play a pivotal role in automating voting systems. This paper explores the potential of using smart contracts for implementing secure and transparent voting mechanisms. The authors propose a model where each vote is treated as a transaction in a smart contract, ensuring the immutability of votes and automatic execution of predefined rules.

The paper outlines how smart contracts can be used to ensure compliance, validate votes, and automatically tally election results without human intervention. Challenges such as scalability and the need for robust smart contract programming to handle complex voting scenarios are discussed, along with potential solutions for making blockchain-based voting systems more efficient.

TITLE: Blockchain-Based Voting: A Practical Implementation Approach

AUTHORS: Singh, A., Thakur, A. (2021)

ABSTRACT:

Blockchain technology is increasingly being explored to make electronic voting systems secure and tamper-proof. This paper presents a practical implementation approach for using blockchain to build a secure voting platform. The authors discuss how blockchain's decentralized structure ensures transparency, security, and non-repudiation of votes. The study emphasizes the advantages of using private blockchains and consensus algorithms to maintain data integrity in the voting process.

The paper also highlights the challenges faced in implementing blockchain-based voting systems, such as ensuring the scalability of blockchain networks, overcoming legal and regulatory issues, and educating the public on how blockchain systems work. Furthermore, the integration of biometric systems like fingerprint and facial recognition is discussed as a way to enhance voter authentication and prevent fraud.

International Journal of
AI Electronics and Nexus Energy
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

TITLE: Face Recognition for Voter Authentication in Blockchain-Based E-Voting Systems

AUTHORS: Kumar, A., Mishra, V. (2022)

ABSTRACT:

This research paper focuses on the integration of face recognition technology into blockchain-based e-voting systems to improve voter authentication. The authors discuss how face recognition can enhance the security of e-voting systems by adding an additional layer of authentication to the voter's identity, ensuring that only authorized individuals can cast votes.

The study also investigates the potential challenges of implementing face recognition systems, including concerns regarding accuracy, privacy, and data security. The authors suggest integrating face recognition with blockchain to provide a seamless and secure voting process while ensuring voter privacy and preventing identity theft.

TITLE: Blockchain and Its Role in Transparency of Voting Systems

AUTHORS: Waghmare, A., Deshmukh, N. (2023)

ABSTRACT:

Blockchain technology is gaining traction as a solution to improve the transparency of voting systems. This paper explores how blockchain can ensure that voting results are tamper-proof, traceable, and verifiable by all stakeholders. The authors discuss the concept of transparency in the context of electronic voting and explain how blockchain can guarantee the integrity of the entire voting process.

The paper also discusses the importance of decentralization in blockchain systems, which prevents any single party from manipulating the voting outcome. Additionally, the authors explore how blockchain can provide a public ledger of all votes cast, ensuring accountability and public trust in the election results.

III. EXISTING SYSTEM

Traditional voting systems often rely on manual processes, electronic voting machines, or online portals without advanced security mechanisms. These systems are susceptible to issues like vote tampering, unauthorized access, and identity fraud. Moreover, the centralized storage of voting data increases the risk of data breaches, compromising the confidentiality and integrity of election results.

IV. PROPOSED SYSTEM

The proposed Smart Voting System combines blockchain technology with fingerprint and facial recognition to ensure a secure, decentralized, and transparent voting process. The system enables voters to register with their biometric and facial data, which is stored on the blockchain for immutable record-keeping. During voting, the system verifies the voter's fingerprint and facial identity before allowing them to cast their vote, thereby eliminating unauthorized access and identity fraud.

V. SYSTEM ARCHITECTURE

The architecture diagram illustrates the overall workflow of the Smart Voting System Using Blockchain, Fingerprint, and Face Recognition. The system consists of three primary entities: the Voter, the Web Application, and the Admin, with Blockchain acting as the secure and immutable storage layer. The web application serves as the central platform that connects voters and administrators while interacting with the blockchain to securely store and retrieve election-related information. This architecture ensures transparency, reliability, and protection against unauthorized modifications.

The voting process begins with the voter registration phase. During registration, the voter provides personal details along with a fingerprint image and a profile photograph. These biometric details are securely processed by the web application and stored in the blockchain, ensuring that the

International Journal of
AI Electronics and Nexus Energy
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

registration records cannot be altered or tampered with. By using blockchain technology, the system maintains an immutable record of registered voters, preventing duplicate registrations and enhancing the overall integrity of the election process.

After successful registration, the voter accesses the system through the login module. Instead of relying solely on usernames and passwords, the system performs fingerprint verification to authenticate the voter. The submitted fingerprint is compared with the encrypted biometric information stored during registration. Only when the fingerprint matches the stored record is the voter granted access to the voting portal. This biometric authentication mechanism significantly reduces the possibility of identity theft, impersonation, and unauthorized access.

Before a voter is allowed to cast a vote, the system performs an additional face recognition verification. The live facial image captured through the camera is compared with the registered profile photograph using a face recognition model. This two-factor biometric authentication, combining fingerprint verification and facial recognition, ensures that only the genuine voter can participate in the election. Once the face is successfully verified, the voter can securely cast a vote, and the voting transaction is immediately recorded on the blockchain, making it permanent and tamper-proof.

The Admin plays a vital role in managing the election process. Through the web application, the administrator can add political parties, register candidate details, manage election information, and monitor vote counts. Administrative operations are securely synchronized with the blockchain to ensure that candidate information and election records remain consistent and cannot be modified maliciously. The administrator cannot alter already recorded votes, thereby preserving election fairness and transparency.

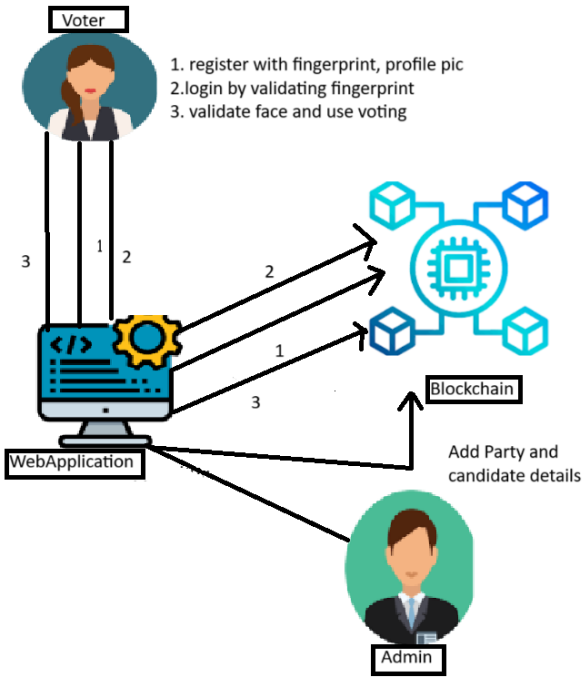

Fig 5.1: System Architecture

VI. IMPLEMENTATION

Fig 6.1: Admin Dashboard

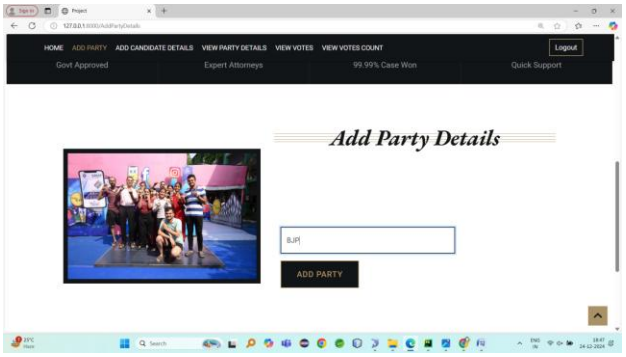

Fig 6.2: Adding Party Details

International Journal of
AI Electronics and Nexus Energy
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

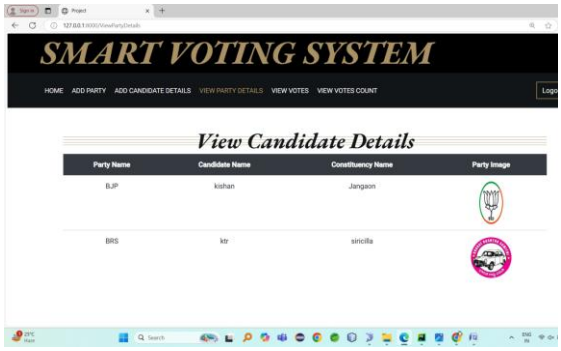

Fig 6.3: View Candidate Details

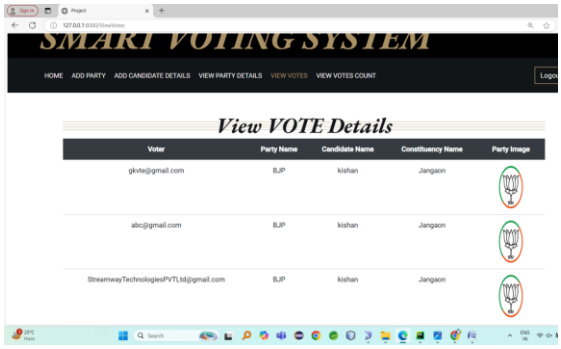

Fig 6.4: View Vote Details

VII. CONCLUSION

The Smart Voting System Using Blockchain, Fingerprint, and Face Recognition successfully addresses the challenges of traditional voting systems by ensuring security, transparency, and voter authenticity. By combining blockchain's decentralized storage with advanced biometric verification methods, the system provides a reliable solution for conducting fair and fraud-proof elections. This innovative approach paves the way for future advancements in secure digital voting systems, contributing significantly to the evolution of democratic processes.

VIII. FUTURE SCOPE

The future scope of the Smart Voting System Using Blockchain, Fingerprint, and Face Recognition focuses on enhancing security, scalability, and accessibility to support large-scale digital elections. Future versions of the system can integrate advanced blockchain platforms with smart contracts to automate the entire election lifecycle, including voter registration, vote validation, and result declaration. This will further improve transparency while minimizing manual intervention and administrative overhead.

The biometric authentication mechanism can be strengthened by incorporating multi-modal biometrics, such as iris recognition and voice authentication, alongside fingerprint and facial recognition. The use of advanced Artificial Intelligence and Deep Learning models can improve the accuracy of face recognition under varying lighting conditions, facial expressions, and aging effects, thereby reducing false acceptance and rejection rates.

The system can also be extended to support remote and mobile voting, enabling eligible citizens to cast their votes securely from any location using smartphones or dedicated voting devices. This enhancement would increase voter participation, particularly for senior citizens, individuals with disabilities, military personnel, and citizens residing abroad, while maintaining high levels of security through blockchain-based verification.

Future implementations may integrate cloud computing and edge computing technologies to improve system scalability and handle millions of voters simultaneously during national elections. Distributed cloud infrastructure combined with blockchain can ensure high availability, fault tolerance, and faster transaction processing, making the system suitable for large-scale governmental elections.

Additional security features such as Zero-Knowledge Proofs (ZKP), Homomorphic Encryption, and Decentralized Identity (DID) can be incorporated to strengthen voter privacy while ensuring vote integrity and anonymity. These cryptographic techniques will allow vote verification without revealing voter identities, thereby enhancing trust and compliance with privacy regulations.

Finally, the system can evolve into a comprehensive national digital election

platform by integrating with government identity databases, digital identity frameworks, and election management systems. Support for multilingual interfaces, real-time election analytics, accessibility features, and interoperability with future blockchain networks will make the platform more inclusive, efficient, and adaptable to the evolving needs of secure electronic voting.

IX. REFERENCES

[1] M. Pawlak, M. Poniszewska-Marańda, and N. Kryvinska, "Towards the Intelligent Edge Computing: Blockchain-Based Smart Voting System," Sensors, vol. 22, no. 4, 2022.
DOI: 10.3390/s22041481

[2] A. Kiayias and G. Panagiotakos, "Speed-Security Tradeoffs in Blockchain-Based Electronic Voting," IET Blockchain, vol. 1, no. 1, pp. 19–26, 2021.
DOI: 10.1049/blc2.12008

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
DOI: 10.48550/arXiv.0807.1099

[4] M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.
DOI: 10.1002/9781119555391

[5] J. Bonneau et al., "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," IEEE Symposium on Security and Privacy, 2015.
DOI: 10.1109/SP.2015.14

[6] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.
DOI: 10.48550/arXiv.2410.11296

[7] A. K. Jain, A. Ross, and K. Nandakumar, Introduction to Biometrics. Springer, 2011.
DOI: 10.1007/978-0-387-77326-1

[8] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4–20, 2004.
DOI: 10.1109/TCSVT.2003.818349

[9] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep Face Recognition," BMVC, 2015.
DOI: 10.5244/C.29.41

[10] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," CVPR, 2015.
DOI: 10.1109/CVPR.2015.7298682

[11] K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," CVPR, 2016.
DOI: 10.1109/CVPR.2016.90

[12] J. Deng, W. Dong, R. Socher, L. J. Li, K. Li, and L. Fei-Fei, "ImageNet: A Large-Scale Hierarchical Image Database," CVPR, 2009.
DOI: 10.1109/CVPR.2009.5206848

[13] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A Survey on Security and Privacy Issues of Blockchain Technology," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 3416–3452, 2020.
DOI: 10.1109/COMST.2020.3015168

[14] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," OSDI, 1999.
DOI: 10.1145/296806.296824

[15] X. Xu, I. Weber, and M. Staples, Architecture for Blockchain Applications. Springer, 2019.
DOI: 10.1007/978-3-030-03035-3