www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 825-831

e-ISSN : 2583-1062
Impact Factor : 7.001

DECENTRALIZED VOTING SYSTEM USING BIOMETRIC AUTHENTICATION

Brijesh A[1], Hitesh Kumar K A[2], Pradeep M[3], Sivaa Ganesh S[4], Dr. S. Pasupathy[5]

[1,2,3,4]UG Student, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamil Nadu, India.

[5]Associate Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamil Nadu, India.

DOI: https://www.doi.org/10.58257/IJPREMS39779

ABSTRACT

Traditional voting systems are prone to voter fraud, tampering, and lack of transparency, leading to distrust in election outcomes. This study investigates a decentralized voting system that integrates blockchain technology and machine learning to enhance security and reliability. The blockchain-based system ensures that votes are securely recorded, immutable, and transparent, preventing manipulation and double voting. Machine learning is utilized for biometric voter authentication and fraud detection, ensuring that only legitimate votes are counted. The system was tested through simulations, demonstrating its effectiveness in preventing unauthorized access and improving election security. Results indicate a significant reduction in fraudulent activities and improved voter verification accuracy. This research highlights the potential of decentralized technology in modern elections, offering a scalable and secure alternative to traditional voting methods. The findings suggest that adopting this system can enhance electoral transparency and public trust, paving the way for more secure and verifiable democratic processes.

Keywords: Blockchain, Machine Learning, Biometric Authentication, Election Security, Decentralized Voting

1. INTRODUCTION

The integrity and security of electoral processes are crucial for maintaining democratic principles. Traditional voting methods, including paper-based ballots (Figure:1) and Electronic Voting Machines (EVMs) (Figure:2), have been widely used in elections worldwide. While EVMs provide a faster and more efficient alternative to manual vote counting, they are still prone to several challenges, such as security vulnerabilities, reliance on centralized data storage, and accessibility issues for voters in remote areas.

Figure:1 Paper-based ballots

Figure:2 Electronic Voting Machines (EVMs)

To address these limitations, researchers have explored the use of blockchain technology for creating a decentralized voting system. Blockchain-based voting ensures transparency, security, and immutability of votes by distributing data across multiple nodes instead of relying on a single central authority. This decentralized approach significantly reduces the risk of vote tampering, hacking, and unauthorized modifications. Additionally, integrating biometric authentication with machine learning enhances voter verification, preventing identity fraud and ensuring that only legitimate votes are counted. Current research in decentralized voting systems focuses on improving scalability, ensuring accessibility for all voters, and enhancing encryption mechanisms to protect voter privacy. By leveraging blockchain's distributed ledger technology, elections can become more secure, verifiable, and resistant to manipulation, ultimately fostering greater public trust in electoral outcomes. This study explores the implementation of a decentralized voting system using blockchain and machine learning to overcome the challenges faced by traditional voting systems.

2. METHODOLOGY

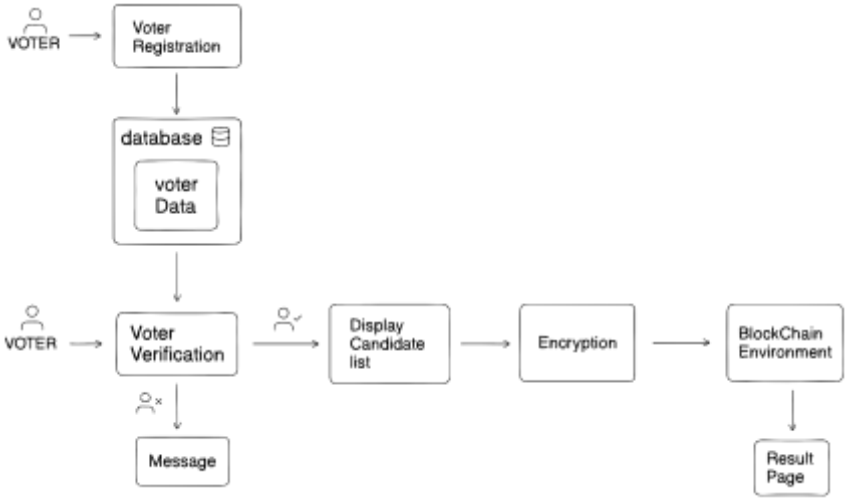
This research implements a Decentralized Voting System using Blockchain and Machine Learning to ensure secure, transparent, and fraud-resistant electoral processes. The methodology is designed to overcome challenges faced by traditional voting systems such as voter fraud, lack of transparency, and manipulation by combining blockchain's immutable ledger with machine learning-based biometric verification. The system follows a modular approach using the Svelte framework for the frontend, ensuring a lightweight and fast user experience.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 825-831

e-ISSN : 2583-1062
Impact Factor : 7.001

2.1 SYSTEM ARCHITECTURE



The system is composed of five primary modules that function in a workflow to ensure end-to-end security and verifiability of the voting process: (Figure:3)

Figure:3 System Architecture

2.1.1 Registration Module

The Registration Module collects essential voter data through a Svelte-based form, including voter ID, age, and facial image. The system checks age eligibility (e.g., 18+) and prevents duplicate registrations. The facial image is processed using machine learning algorithms to extract facial features, which are securely stored in a database for future verification. This module forms the foundation for voter authentication and ensures that only eligible users can access the system. The user interface is intuitive and responsive, enhancing user experience. By digitizing voter onboarding, the module minimizes human error and promotes a trusted voter list. It also prepares the system for a secure and AI-assisted verification phase by building a clean dataset of eligible voters with unique biometric records, ensuring high accuracy during elections. (Figure:4)

Figure:4 Registration Module

2.1.2 Voter Verification Module

The Voter Verification Module plays a crucial role in ensuring the security and integrity of the voting process. It uses real-time facial recognition to verify the voter's identity. A live image is captured from the user and compared against the pre-registered image using cosine similarity, a machine learning technique to measure the similarity between facial feature vectors. A score near 1 indicates a close match, confirming the user's identity and allowing them to proceed. This eliminates the chances of impersonation or unauthorized access. The module is designed to detect spoofing and prevent fraudulent activity. Integrated with a Svelte frontend, it offers a seamless user experience. It is the first line of defense in the system and ensures that only legitimate voters enter the actual voting interface, thereby enhancing both trust and authentication accuracy. (Figure:5)

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 825-831
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Figure:5 Voter Verification Module

2.1.3 Candidate List Module

The Candidate List Module ensures that voters can make informed choices securely. Once a voter is verified, this module fetches the list of candidates stored on the blockchain via smart contracts written in Solidity. These smart contracts ensure that the candidate list remains immutable and tamper-proof. The Svelte-based frontend presents the list clearly, allowing users to browse and select their preferred candidate. (Figure:6)

Before vote submission, the system checks whether the voter has already cast a vote. If so, a message is displayed on the UI indicating: "Already voted."(Figure:8) This prevents multiple voting attempts and reinforces trust in the system.

If the voter is eligible, their selection is immediately encrypted and submitted to the blockchain. Upon successful submission, a confirmation message is shown: "Vote successfully casted."(Figure:7) This ensures the user is informed of the outcome while maintaining voter privacy.

By utilizing blockchain to store and retrieve candidate data, this module guarantees that no unauthorized changes can be made to the list, thus maintaining election integrity. The secure, dynamic retrieval of candidates ensures real-time accuracy and fairness in every voting session while building confidence in the system's transparency and structure.

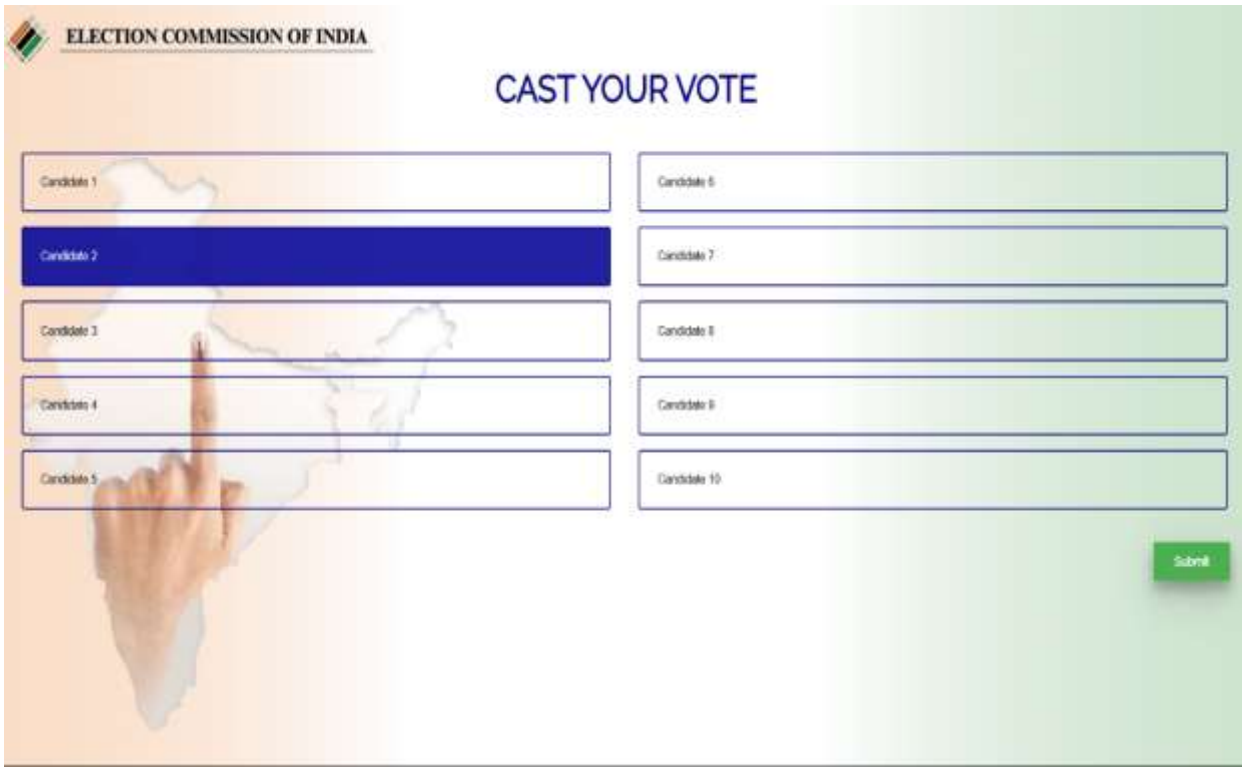


Figure:6 Candidate List

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 825-831
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

Figure:7 If new voter votes

Figure:8 If already voted

2.1.4 Encryption Module

The Encryption Module is essential for maintaining the confidentiality and security of each vote cast in the system. Once a user selects a candidate, the vote is passed through this module, which uses robust encryption algorithms to encode the vote before it is recorded on the blockchain. This process ensures that the vote cannot be read, traced, or altered by any intermediary. Even system administrators cannot access or identify individual votes. Encryption also prevents replay attacks or data tampering during transmission. The module works seamlessly in the background and integrates with the blockchain module to ensure that only encrypted votes are pushed onto the ledger. By guaranteeing data integrity and voter anonymity, the encryption module strengthens the overall trust in the decentralized voting system and upholds democratic principles in a secure digital form.

2.1.5 Blockchain Module

The Blockchain Module is the foundation of the decentralized voting system. It stores all encrypted votes using smart contracts on a blockchain network, ensuring that data is immutable, transparent, and decentralized. Once a voter's encrypted vote is submitted, it becomes a part of the distributed ledger, making it resistant to tampering, deletion, or unauthorized modification.

Smart contracts handle the vote submission process, ensuring that rules such as one vote per user are enforced automatically. This module eliminates the need for a central authority and makes the voting process trustless everyone can verify the outcome independently. Each transaction (vote) is timestamped, verifiable, and securely stored, promoting accountability.

During development and testing, the system uses Ganache Workspace (Figure:9), a local Ethereum blockchain, to simulate real blockchain behaviour. This allows for secure testing of smart contracts, quick debugging, and accurate transaction flow analysis before deployment to a live network.

The integration with the encryption module ensures that while the votes are visible on the chain, their content remains confidential, reinforcing both transparency and privacy.

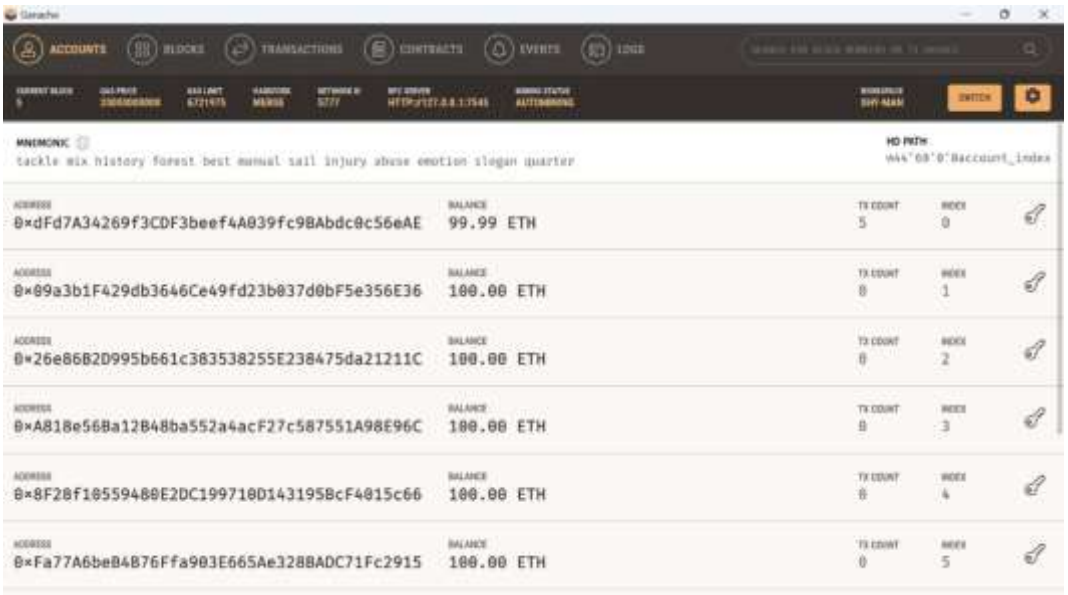


Figure:9 Ganache Workspace

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 825-831

e-ISSN : 2583-1062
Impact Factor : 7.001

2.1.6 Result Module

The Result Module is responsible for retrieving, decrypting, and tallying votes after the election concludes. It pulls encrypted votes directly from the blockchain and processes them through secure decryption algorithms. Once decrypted, the module counts each vote accurately and maps it back to the respective candidate. The final result is displayed on a Svelte frontend using visual elements like graphs or tables for clarity (Figure:10). Since all data comes from an immutable blockchain ledger, the results are fully verifiable and tamper-proof. This fosters public trust, as third-party auditors can cross-verify the vote count without accessing individual voter identities. The module also supports real-time result computation if needed and guarantees that the election process remains fair, transparent, and auditable, meeting the core goals of decentralization and democratic accountability.

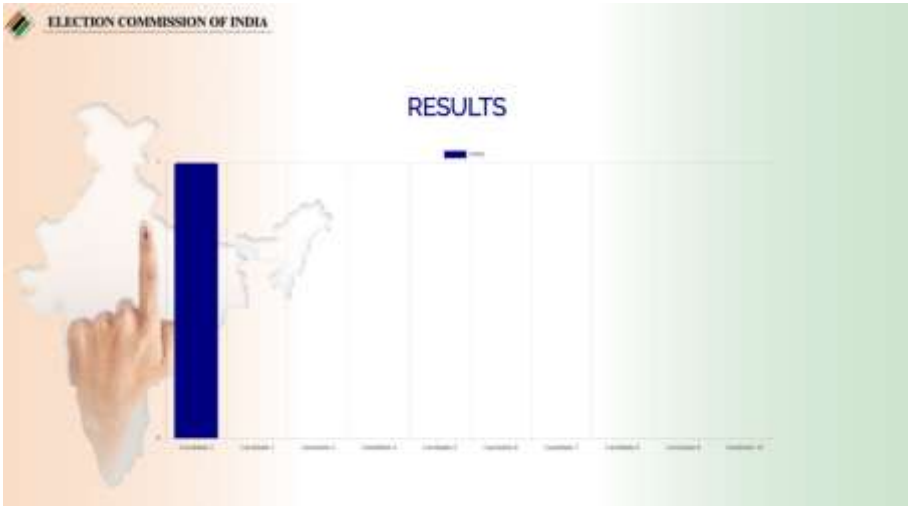


Figure:10 Result Page

2.2 TECHNOLOGY STACK AND TOOLS USED

2.2.1 Blockchain Platform:

Ethereum - used for securely recording and managing votes; tested locally using the Ganache workspace for simulating blockchain networks.

2.2.2 Smart Contracts:

Developed using Solidity, enabling automated vote handling, candidate listing, and immutable storage of encrypted vote data on the blockchain.

2.2.3 Facial Recognition:

Facial recognition using ArcFace extracts highly discriminative facial embeddings by optimizing angular margin loss. Comparison is done using cosine similarity to measure the closeness between feature vectors for identity verification.

2.2.4 Frontend:

Built using Svelte, a modern JavaScript framework that compiles to highly efficient code, ensuring fast, reactive, and lightweight user interfaces for registration, voting, and result viewing.

2.2.5 Backend:

Developed using Flask, a Python-based micro web framework responsible for handling facial recognition processing, data validation, and interaction between the Svelte frontend and Ethereum blockchain.

2.2.6 Database:

MongoDB – A NoSQL document-oriented database used to store voter profiles, biometric metadata and flexible format.

3. SECURITY ANALYSIS

The Decentralized Voting System using Biometric Authentication is designed with robust security mechanisms to protect against various vulnerabilities. Below is an analysis of how the system addresses common security threats:

3.1 Identity Spoofing Attempts

The system uses facial recognition as a biometric authentication method (using ArcFace), which ensures that only the genuine voter can access the system. Advanced face detection models prevent spoofing using photographs or videos. Additionally, liveness detection (using YOLO model) techniques can be integrated to further enhance protection against impersonation.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 825-831
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

3.2 Vote Tampering Risks

Votes are recorded on the blockchain, ensuring immutability and transparency. Once a vote is cast, it is encrypted and added to a block, which is then validated by the network. This makes any form of tampering virtually impossible without altering the entire blockchain, which is computationally infeasible.

3.3 Data Breach Scenarios

All sensitive data such as biometric details are either not stored or securely encrypted during transmission. Voter identity is verified in real-time and not permanently stored in any centralized server, reducing the attack surface for data breaches. Votes are anonymized before recording to maintain voter privacy.

3.4 Replay Attacks

Replay attacks are prevented by generating a unique token for each voting session. The system verifies the freshness of the request using timestamps or nonce values, ensuring that previously captured requests cannot be reused to manipulate voting outcomes.

4. FUTURE SCOPE

- **Aadhaar Integration**: The system can be integrated with Aadhaar or other government ID databases to ensure voter authenticity and eliminate duplicate or fake registrations.
- **Multi-modal Biometrics**: Future versions can include support for multi-modal biometric authentication such as fingerprint, facial recognition, enhancing security and reliability.
- **Public Blockchain Deployment**: Moving from a private to a public blockchain infrastructure will enable transparent, decentralized voting accessible to a wider audience while maintaining data integrity.
- **Mobile Voting Platforms**: A mobile-friendly, secure voting platform can allow remote participation from anywhere, helping NRIs, senior citizens, and physically challenged voters to cast their votes conveniently.

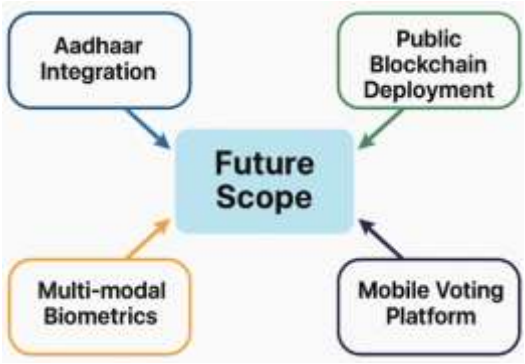


Figure:11

5. CONCLUSION

This research presents a decentralized voting system that upholds transparency, security, and voter privacy by integrating facial recognition and blockchain technology. Through real-time authentication using cosine similarity, the system ensures that only eligible individuals can cast their votes. Encryption of votes prior to submission, coupled with blockchain's immutable storage, safeguards voter data and prevents manipulation or duplication.

Smart contracts automate the management of candidate lists and vote recording, enforcing integrity and eliminating manual intervention. The result module strengthens credibility by securely retrieving, decrypting, and transparently displaying election outcomes. By eliminating reliance on a central authority, this system effectively addresses challenges such as fraud, vote tampering, and lack of trust.

Overall, the methodology lays a robust foundation for secure, fair, and democratic digital voting systems, demonstrating a viable solution for future electoral frameworks.

6. REFERENCES

[1] Donovan Gentles, Suresh Sankaranarayanan, Application of Biometrics in Mobile Voting, I.J. Computer Network and Information Security, Vol. 7, July 2012, pp. 57–68.

[2] Dylan Yaga, Peter Mell, Nik Roby, Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NISTIR 8202, October 2018.

[3] Jun Huang, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, Kim-Kwang Raymond Choo, "The Application of the Blockchain Technology in Voting Systems: A Review," ACM Computing Surveys (CSUR), Vol. 54, Issue 3, Article No. 60, pp. 1–28, 2021.

[4] Uzma Jafar, Mohd Juzaiddin Ab Aziz, and Zarina Shukur, “Blockchain for Electronic Voting System Review and Open Research Challenges,” Sensors, Vol. 21, No. 17, 2021, Article 5874.

[5] Eduardo Takeo Ueda, Marcelo Moro Da Silva, Anderson A. A. Silva, Norisvaldo Ferraz Junior, Fabio Dacêncio Pereira, Alessandro Santiago dos Santos, Adilson E. Guelfi, and Sergio Takeo Kofuji, "A Proposed Blockchain-Based Voting System with User Authentication through Biometrics," Journal of Information Security and Cryptography (Enigma), vol. 8, no. 1, pp. 1–11, Sep. 2021.

[6] Pooja S, Laiju K. Raju, Utkarsh Chhapekar, and Chandrakala C.B., "Face Detection using Deep Learning to ensure a Coercion Resistant Blockchain-based Electronic Voting," Engineered Science, vol. 16, pp. 341–353, 2021.

[7] Md Jobair Hossain Faruk, Mazharul Islam, Fazlul Alam, and Hossain Shahriar, “BieVote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework,” March 2022, ResearchGate.

[8] Abhay Singh, Ankush Ganesh, Rutuja Rajendra Patil, Sumit Kumar, Ruchi Rani, and Sanjeev Kumar Pippal, “Secure Voting Website Using Ethereum and Smart Contracts,” Applied System Innovation, vol. 6, no. 4, p. 70, 2023.