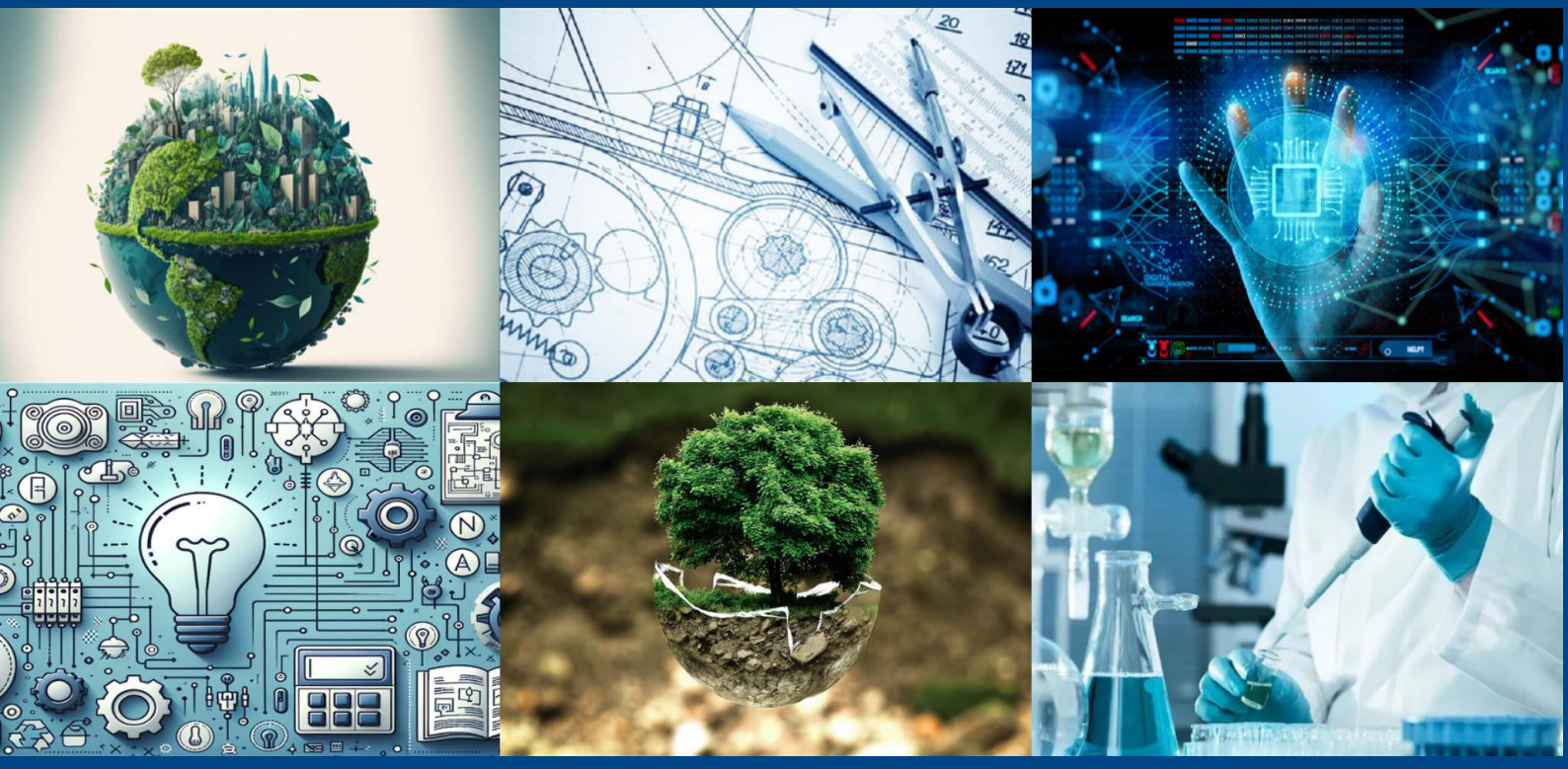
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 8, Issue 5, May 2025**

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805082

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Online Voting System using Blockchain

Prof. Sushma Mule [*1], Siddhi Kondhalkar [*2], Sarvada Choudhari [*3], Samruddhi Deshmukh [*4], Sana Shaikh [*5], Pranali Jadhav [*6]

Professor, Department of Computer Science and Engineering, MIT College of Railway Engineering and Research, Barshi, Maharashtra, India[*1]

Student, Department of Computer Science and Engineering, MIT College of Railway Engineering and Research, Barshi, Maharashtra, India[*2-*6]

ABSTRACT: This study presents a secure and decentralized online voting system that leverages blockchain technology integrated with Aadhaar and iris-based biometric authentication. Utilizing Ethereum smart contracts, the system ensures voter eligibility by matching iris scan data hashed via SHA-256 with pre-verified Aadhaar-linked hashes. It eliminates duplicate registrations and enhances integrity through tamper-proof transparent vote recording on the blockchain. Candidate details, including images and party affiliations, are stored via the IPFS, ensuring decentralized accessibility. The front end was developed using React.js, while the backend iris verification was performed using Flask, OpenCV, and MediaPipe. The entire voting lifecycle, from voter registration, login, to final vote casting, is governed by smart contract logic, ensuring one-person-one-vote, secure election timing, and transparency in vote counts. Compared with India's existing EVM-based system, this method offers enhanced transparency, biometric-level voter validation, and immutable audit trails, minimizing the scope for fraud or impersonation. Our system architecture and experimental results demonstrate improved efficiency and security compared to traditional methods, providing a viable framework for future digital elections in India and beyond.

KEYWORDS: Blockchain Voting, Aadhaar Authentication, Iris Recognition, Ethereum Smart Contracts, IPFS, Secure e-Voting, Biometric Verification, Decentralized Elections, SHA-256 Hashing, Web3.js.

I. INTRODUCTION

Conducting secure, transparent, and accessible elections is the cornerstone of democratic governance. However, traditional voting systems, such as those employed in India, often face challenges, including voter impersonation, tampering, limited accessibility for remote populations, and logistical inefficiencies. These issues undermine public trust and hinder voters' participation. With the increasing demand for digital transformation and enhanced security, recent research has turned to advanced technologies to build more robust, transparent, and inclusive voting infrastructure.

Blockchain technology, renowned for its decentralized and tamper-resistant architecture, has emerged as a promising solution for addressing the critical challenges of traditional electoral systems. Its immutable ledger ensures that once a vote is cast, it cannot be altered, thus fostering voter confidence and process transparency. Simultaneously, biometric technologies such as iris recognition offer highly accurate and fraud-resistant identity verification, making them ideal for securing digital identities in sensitive applications such as voting.

This paper presents the design and implementation of a secure online voting system that integrates three core technologies: Ethereum-based smart contracts for secure and verifiable vote recording, Aadhaar-based identity validation for national linkage and voter uniqueness, and iris biometric authentication for two-factor verification. By leveraging smart contracts, the system automates vote tallying and enforces "one person, one vote" logic while ensuring that no vote can be manipulated or duplicated. The iris scan, hashed, and compared via a backend system, ensures that only the legitimate Aadhaar holder can vote.

Furthermore, the IPFS is used to store candidate data, such as images, ensuring decentralized and publicly auditable access. This fusion of blockchain, Iris Authentication, and national ID authentication not only enhances electoral

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

integrity, but also paves the way for secure, scalable, and remote voting—particularly crucial in times of pandemic or for non-resident voters. The proposed model represents a significant step toward trustworthy digital-first democratic systems.

II. METHODOLOGY

The methodology adopted for the project "Blockchain-based Online Voting System with Aadhaar and Iris Authentication" integrates blockchain technology, Aadhaar-based verification, and biometric iris recognition to ensure a secure, transparent, and tamper-resistant voting experience. This section outlines the techniques, system design, and analysis used to implement and evaluate the proposed solution.

1.1 System Architecture and Design

The proposed system comprises three major modules: the front-end interface, backend authentication engine, and Ethereum blockchain smart contract. The front-end, developed using React.js, provides a seamless interface for voter registration, login, and voting. The backend, built using Flask, integrates OpenCV and MediaPipe to capture and verify the iris image. The Aadhaar number was inputted by the user and verified in conjunction with the iris scan. Once verified, the smart contract deployed on the Ethereum test network using Hardhat is invoked to register or log in the voter.

1.2 Iris Authentication and Aadhaar Verification

Users initiate registration by submitting their Aadhaar number and capturing an iris image using a webcam. The image was pre-processed, hashed using the SHA-256 algorithm, and matched with the stored data for verification. During the login, a similar process is followed to authenticate the voter. The system ensures that each Aadhaar is registered only once and voting can be performed only after successful verification.

1.3 Smart Contract Voting Logic

Smart contracts govern the voting processes. Admins initialize the election by adding candidates and setting time constraints. Registered users can view candidate profiles (names, parties, and IPFS-hosted images) and cast immutable votes. The smart contract enforces voting rules, prevents double voting, and ensures integrity through decentralized recordkeeping.

1.4 Security & Validation Measures

Security is enforced through two-factor authentication (Aadhaar and iris scans), SHA-256 hashing to prevent biometric leakage, and blockchain-based immutability. The system was validated through functional testing, scenario-based voting attempts, and a comparison of vote counts before and after each transaction.

III. MODELING AND ANALYSIS

The proposed system architecture follows a Model-View-Controller (MVC) design pattern to ensure separation of concerns and maintainability. The system is divided into three primary components:

View:
The user interface is developed using React.js and serves as the View layer. It facilitates user interaction by providing intuitive screens for registration, login, voting, and result display. This front-end communicates with both the smart contract backend and the Python-Flask-based biometric verification system.

Controller:
The controller layer acts as the logic handler for user and admin activities. For users, it handles Aadhaar number submission, iris scan capture, and verification through a Flask-based API using OpenCV and MediaPipe. Upon successful validation, it interacts with Ethereum smart contracts to register voters, handle login, and enable vote casting. For administrators, it manages candidate entry, election start/stop, and result generation.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805082

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Model:
The model component includes the decentralized storage and smart contract state. It maintains critical datasets such as voter registration (via Aadhaar + hashed iris), candidate information (name, party, IPFS image hash), and vote counts. Data integrity is ensured through blockchain immutability, while IPFS guarantees decentralized storage of visual content.

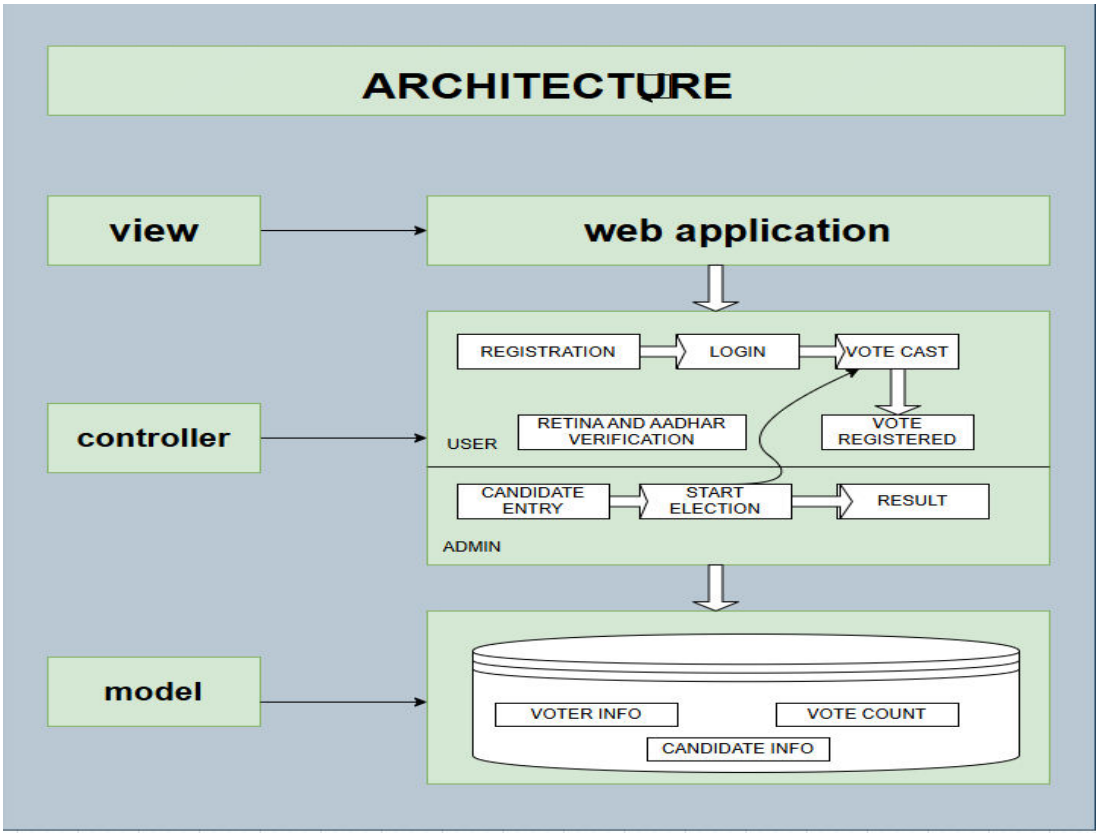


Figure 1: MVC-Based Architecture of the Web-Based Online Voting System

This layered approach enables secure, modular development and transparent voting operations. The model ensures tamper-proof data, the controller governs logic flow and validation, and the view provides accessibility to all stakeholders.

IV. RESULTS AND DISCUSSION

Result:
The proposed system was developed using a modular architecture integrating front-end, back-end, and blockchain technologies as described earlier. The implementation phase followed the design principles to ensure secure, authenticated, and tamper-proof online voting. Each stage of the system was tested thoroughly to validate functionality and robustness. The results are discussed below along with corresponding interface screenshots.

1. User Registration with Aadhaar and Iris Authentication
The registration interface allows the user to input their Aadhaar number and capture an iris image via a webcam. The iris is processed using MediaPipe and OpenCV in a Python Flask backend, and the resulting hash is stored after validation. A successful match allows the user to be registered on the Ethereum smart contract through Web3.js.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805082

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Figure 2: Registration Interface with Iris Capture

2. Secure Voter Login

For authentication, users log in using their Aadhaar number and a real-time iris scan. The hash of the current iris is compared with the stored hash on the blockchain. Only a match allows further access. This step demonstrates the effectiveness of the two-factor authentication approach.

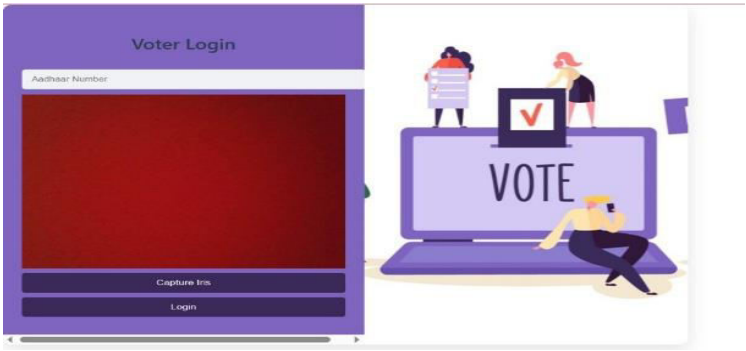


Figure 3: Login Interface with Iris Verification

3. Voting Interface and Blockchain Interaction

Once authenticated, users are redirected to the voting page where candidate profiles are displayed along with their IPFS-hosted images and party names. The voter selects a candidate, and the vote is immutably recorded on the blockchain.

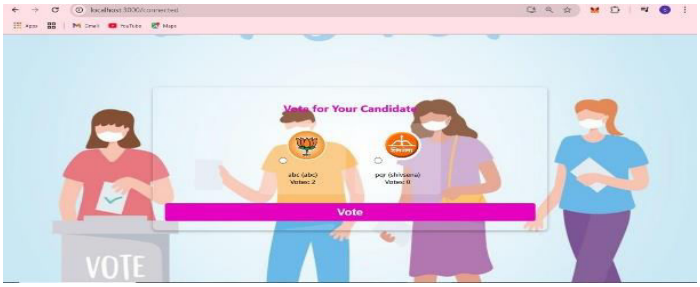


Figure 4: Voting Page Displaying Candidates

4. Vote Confirmation and Tally

After casting a vote, the system displays a confirmation message. The backend verifies whether the vote count for the selected candidate has increased by one. This provides real-time feedback and builds trust in the process.

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805082

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Figure 5: Vote Confirmation Message

5. Admin Interface and Results Display

An admin panel allows election control including start/end of election and candidate management. Once voting ends, the results are displayed showing the candidate with the highest votes. In case of a tie, appropriate messages are shown.

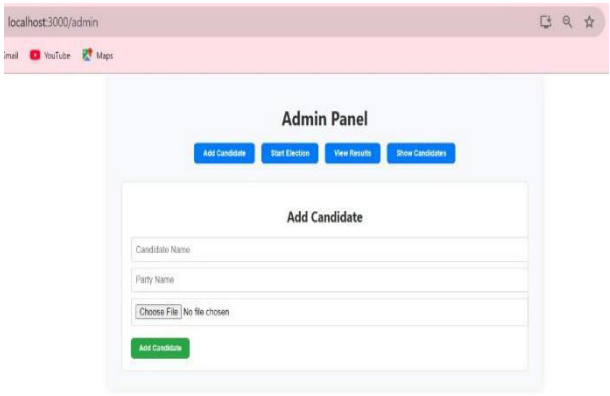


Figure 6: Admin Panel and Add Candidate

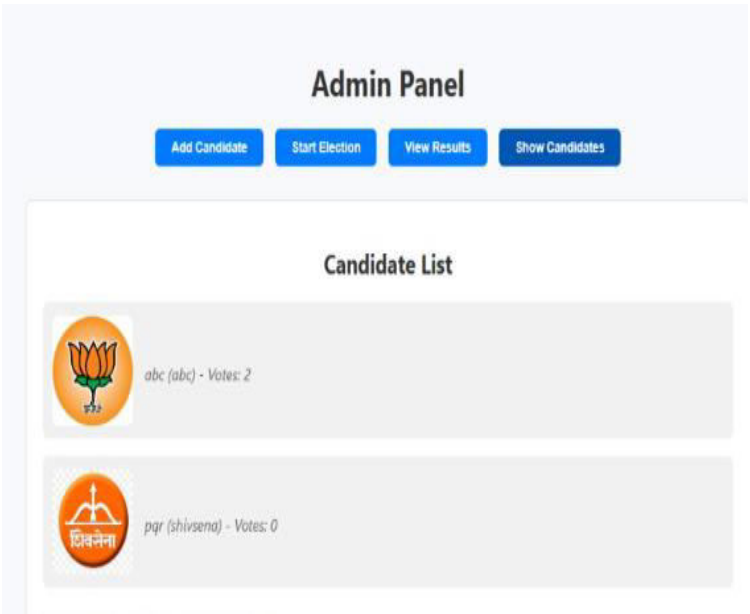


Figure 7: Admin Panel and Candidate List

© 2025 IJMRSET | Volume 8, Issue 5, May 2025| DOI:10.15680/IJMRSET.2025.0805082

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

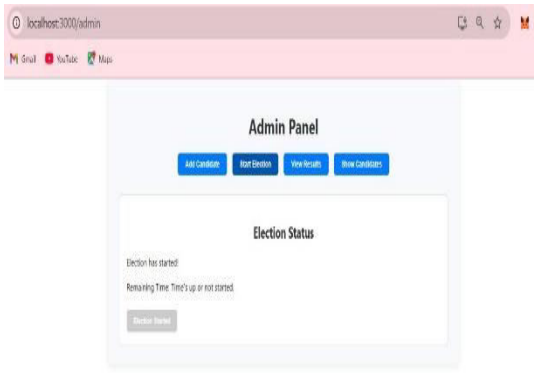


Figure 8: Admin Panel and Election Status

Figure 9: Admin Panel and Election Result

Discussion:

The system demonstrates successful integration of blockchain and biometric authentication, ensuring end-to-end security and transparency. Compared to the traditional Indian voting system, which involves EVMs and manual verification, this approach offers faster results, better accessibility, and reduced risk of fraud. Each action is logged on the blockchain, ensuring immutability and auditability.

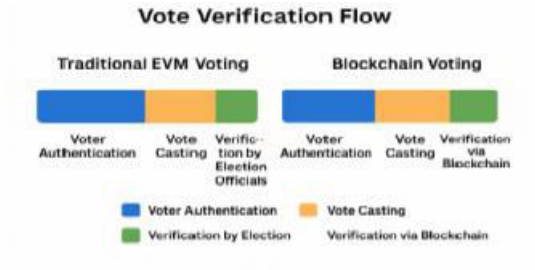


Figure 7: Vote Verification Flow

V. CONCLUSION

This research has successfully developed a secure and transparent online voting system using a combination of blockchain technology, Aadhaar-based identity verification, and iris recognition for biometric authentication. The integration of Ethereum smart contracts ensures immutability and traceability of each vote, addressing core issues like tampering, multiple voting, and lack of transparency often found in traditional systems.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

The system architecture effectively balances user accessibility with high security, leveraging IPFS for decentralized image storage and SHA-256 hashing to protect biometric data. Each component-from registration to final vote casting was designed to enforce a one-person-one-vote principle while maintaining privacy and trust in the process.
The implementation demonstrates that advanced technologies, when used together thoughtfully, can overcome the logistical inefficiencies and vulnerabilities in conventional voting mechanisms. The project contributes to the vision of building future-ready, scalable, and tamper-resistant electoral systems. Future scope includes extending support for offline voting, wider biometric coverage, and integration with government election bodies for broader deployment.

VI. ACKNOWLEDGEMENTS

We would like to express our heartfelt gratitude to all those who have supported and guided us throughout the course of this project. The successful completion of this research work is a reflection of the collective effort, encouragement, and knowledge imparted to us by our mentors and well-wishers.

We are deeply grateful to our esteemed project guide, **Prof. Sushma Mule**, for her invaluable guidance, constant encouragement, and insightful suggestions at every stage of our work. Her mentorship has played a pivotal role in shaping the direction and quality of this research.

We extend our sincere thanks to **Prof. S.S. Mule**, Head of the Department, Computer Science and Engineering, for his consistent support and for providing a conducive environment for academic research. We are equally thankful to **Dr. M.J. Lengare**, Principal of our institute, for his motivation and encouragement throughout the project duration.
We also take this opportunity to acknowledge the entire CSE department faculty for their technical assistance, timely feedback, and moral support, which greatly contributed to our learning and success.
Finally, we would like to thank our parents and friends for their unwavering support, encouragement, and understanding, which kept us motivated and focused throughout this endeavor.

REFERENCES

[1] Muhammad Asaad Cheema, Nouman Ashraf, Asad Aftab “Machine Learning with Blockchain for Secure E-voting System”, IEEE Access, pp. 978-1-7281-7407,2020
[2] Sathya V, Arpan Sarkar, Aritra Paul, “ Blockchain Based Cloud Computing Model on EVM Transactions for Secure Voting”, IEEE Access, 978-1-5386-7808-4 ,2019 Gyusoo Kim and Seulgi Lee, “2014 Payment Research”, Bank of Korea, Vol. 2015, No. 1, Jan. 2015.
[3] T. Dimitriou, “Efficient, coercion-free and universally verifiable blockchain-based voting,” Computer Networks, vol. 174, p. 107234, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619317414
[4] Hui Yang, Haowei Zheng, Jie Zhang, Yizhen Wu, Young Lee, Yuefeng Ji,”Blockchain-based Trusted Authentication in Cloud Radio over Fiber Network for 5G”, 2017 16th International Conference on Optical Communications and Networks (ICOCN)
[5] Shifa Manaruliesya Anggriane, Surya Michrandi Nasution, Fairuz Azmi,”Advanced E-Voting System Using Paillier Homomorphic Encryption Algorithm”, 2016 International Conference on Informatics and Computing (ICIC)
[6] Haijun Pan, Edwin Hou, Senior Member, and Nirwan Ansari, Fellow,”M-NOTE: A Multi-part Ballot based E-voting System with Clash Attack Protection”, IEEE ICC 2015 - Communication and Information Systems Security Symposium
[7] Pierro, Massimo Di. ”What Is the Blockchain?.” Computing in Science & Engineering 19, no. 5 (2017): 92-95.
[8] Hanifatunnisa, Rifa, and Budi Rahardjo. ”Blockchain based e-voting recording system design.” In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1 6. IEEE, 2017.
[9] Aste, Tomaso, Paolo Tasca, and Tiziana Di Matteo. ”Blockchain tech nologies: The foreseeable impact on society and industry.” computer 50, no. 9 (2017): 18-28.
[10] Liu, Yi, and Qi Wang. ”An E-voting Protocol Based on Blockchain.” IACR Cryptology ePrint Archive 2017 (2017): 1043.
[11] Dagher, Gaby G., Praneeth Babu Marella, Matea Milojkovic, and Jordan Mohler. ”BroncoVote: Secure Voting System Using Ethereums Blockchain.” (2018).

[12] Chatterjee, Rishav, and Rajdeep Chatterjee. ”An Overview of the Emerging Technology: Blockchain.” In Computational Intelligence and Networks (CINE), 2017 3rd International Conference on, pp. 126-127. IEEE, 2017.

[13] Nayak, Arpita, and Kaustubh Dutta. ”Blockchain: The perfect data protection tool.” In Intelligent Computing and Control (I2C2), 2017 International Conference on, pp. 1-3. IEEE, 2017.

[14] Mirzayi, Sahar, and Mohammad Mehrzad. ”Bitcoin, an SWOT analysis.” In Computer and Knowledge Engineering (ICCKE), 2017 7th Interna tional Conference on, pp. 205-210. IEEE, 2017.

[15] Khoury, David, Elie F. Kfoury, Ali Kassem, and Hamza Harb. ”Decen tralized Voting Platform Based on Ethereum Blockchain.” In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1-6. IEEE, 2018.

[16] Wst, Karl, and Arthur Gervais. ”Do you need a Blockchain?.” In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45 54. IEEE, 2018

[17] Lee, Kibin, Joshua I. James, Tekachew G. Ejeta, and Hyoung J. Kim. ”Electronic voting service using block-chain.” Journal of Digital Forensics, Security and Law 11, no. 2 (2016): 8.

[18] eber, Ingo, Vincent Gramoli, Alex Ponomarev, Mark Staples, Ralph Holz, An Binh Tran, and Paul Rimba. ”On availability for blockchain based systems.” In Reliable Distributed Systems (SRDS), 2017 IEEE 36th Symposium on, pp. 64-73. IEEE, 2017.

[19] P. McCorry, S. F. Shahandashti, and F. Hao, “A smart contract for board room voting with maximum voter privacy,” in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[20] Y.Li, W. Susilo, G. Yang, Y. Yu, D. Liu, and M. Guizani, “A blockchain based self-tallying voting scheme in decentralized iot,” arXiv preprint arXiv:1902.03710, 2019.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com