Decentralized Voting using Ethereum based Blockchain, IoT, and Facial Recognition with EVM Ecosystem

Omprakash A. Jaisinghani
Department of C.S.E,
H.V.P.M's College of Engineering & Technology
Amravati (M.S), India

Prabhakar L. Ramteke
Department of C.S.E,
H.V.P.M's College of Engineering & Technology
Amravati (M.S), India

Abstract

India‟s electoral system, the world‟s largest democracy, faces persistent challenges in ensuring secure, transparent, and tamper-proof voting processes. While Electronic Voting Machines (EVMs) have streamlined elections since the 1990s, concerns over tampering, voter fraud, and lack of auditability remain unresolved. This research proposes a novel blockchain-integrated electronic voting system enhanced with IoT devices and Aadhaar-based facial recognition to address these shortcomings. The system leverages Ethereum blockchain technology to create an immutable, decentralized ledger for vote storage, ensuring transparency and resistance to manipulation. IoT sensors monitor EVMs in real-time, detecting physical tampering, while Aadhaar-linked biometric authentication prevents impersonation and duplicate voting. A Local Binary Pattern Histogram (LBPH) algorithm validates voter identities through facial recognition. The framework employs AES-256 and SHA-256 encryption to secure voter data and integrates smart contracts for automated vote tallying. By combining blockchain‟s decentralization, biometric authentication, and IoT-enabled monitoring, this system offers a robust solution to electoral vulnerabilities, enhancing public trust and operational efficiency. The study concludes with recommendations for scaling the solution, including machine learning optimizations and hybrid blockchain architectures for large-scale deployment.

Keywords— Blockchain based Electronic Voting Machine, Secure Voting mechanism using Internet of Things (IoT), Ethereum-based Voting Machine.

I. INTRODUCTION

Voting is the cornerstone of democratic governance, enabling citizens to shape their political landscape. In India, with over 900 million eligible voters, the integrity of elections is paramount. However, traditional voting methods from paper ballots to Electronic Voting Machines (EVMs) struggle with systemic flaws. Paper-based systems are prone to manual errors and fraud, while EVMs, despite streamlining the process, face allegations of tampering, lack of verifiable audit trails, and susceptibility to physical attacks. These challenges undermine public trust and risk the legitimacy of electoral outcomes. As technology evolves, there is an urgent need to reimaging voting systems with security, transparency, and accessibility at their core. The digitization of voting processes has introduced electronic solutions, yet vulnerabilities persist. EVMs, though efficient, operate on centralized architectures, creating single points of failure. Reports of booth capturing, vote manipulation and malfunctioning machines highlight critical gaps. For instance, brief physical access to an EVM allows malicious actors with basic electronics knowledge to alter results. Furthermore, manual voter authentication remains error-prone, enabling impersonation and duplicate voting. These issues demand a paradigm shift toward decentralized, auditable systems that empower voters and authorities [1], [5].

Blockchain technology, renowned for its immutable and transparent ledger system, offers a transformative solution. Originally developed for cryptocurrency transactions, blockchain‟s decentralized structure ensures no single entity controls the data, making it inherently resistant to tampering. Each vote, recorded as a cryptographically linked block, creates an unbreakable chain of custody [2]. When integrated with IoT devices, blockchain can monitor EVM operations in real-time, flagging anomalies like unauthorized access. Complementing this, biometric authentication using India‟s Aadhaar database a repository of 1.3 billion citizens‟ demographic and biometric data ensures only eligible voters participate. Facial recognition algorithms, such as LBPH, add another layer of security by matching live captures with stored profiles, minimizing identity fraud [10]. This research presents a holistic framework that synergizes blockchain, IoT, and Aadhaar-based authentication to address electoral vulnerabilities. The system employs Ethereum smart contracts to automate vote recording and tallying, eliminating human intervention in result computation. IoT sensors embedded in EVMs transmit real-time operational data to a decentralized network, enabling swift detection of hardware tampering [3]. Aadhaar integration ensures one-vote-per-voter compliance, while SHA-256 and AES-256 encryption safeguard data integrity. A pilot implementation using Raspberry Pi Pico hardware and Ganache blockchain servers validated the system‟s efficacy, demonstrating tamper-proof vote storage and rapid result generation [12], [15].

The proposed system‟s innovation lies in its multi-layered approach. First, it replaces centralized EVM databases with a blockchain ledger, allowing voters to independently verify their votes via transaction hashes. Second, biometric authentication coupled with IoT-driven monitoring mitigates risks of booth capturing and hardware manipulation [4]. Third, cost-effective encryption protocols ensure scalability without compromising security. Preliminary tests show the system reduces result declaration time by 75% compared to manual methods while maintaining 100% accuracy in vote counts [11], [14]. These advancements address longstanding critiques of India‟s electoral process, offering a blueprint for secure, transparent, and inclusive elections. In the following sections, we detail the system‟s architecture, including blockchain configuration, facial recognition workflows, and IoT integration. We analyze experimental results from prototype deployments, discuss comparative advantages over existing solutions, and outline future research directions. By bridging technological innovation with electoral governance, this study aims to fortify democratic processes against emerging threats, setting a global benchmark for trustworthy voting systems[1],[13].

II. LITERATURE REVIEW

S. T. Alvi et al. propose traditional voting systems, including EVMs and mobile voting, face challenges like tampering, centralization, and insufficient anonymity. Blockchain technology offers decentralized, immutable solutions, as seen in Bitcoin and Ethereum‟s smart contracts. This paper integrates blockchain, BioHash, and smart contracts to address these gaps. The proposed system ensures anonymity (via public keys), integrity (Merkle trees), and singularity (smart contract-based anti-duplication), while optimizing speed through selective miner nomination. Author also highlights its superiority in verifiability, decentralization, and resistance to Sybil/51% attacks over prior works like mobile voting. Future work focuses on quantum-resistant encryption [6].

S. V. Oprea et al. propose traditional e-voting systems face challenges such as security vulnerabilities, lack of transparency, and scalability, particularly in university elections where voter turnout and trust are critical. Blockchain technology has been explored to address these issues, with platforms like Ethereum and Hyperledger offering decentralized solutions (Nakamoto, 2009; Buterin, 2015). However, distributed consensus mechanisms often introduce complexity and latency, making them impractical for smaller-scale elections. Prior blockchain-based voting systems, such as Voatz, faced criticism for security flaws and centralization risks, while others emphasized End-to-End Verifiability (E2E-V) but struggled with usability. This paper proposes a blockchain table-based architecture tailored for university elections, prioritizing simplicity and efficiency. Unlike distributed blockchains, it leverages Oracle‟s blockchain tables—immutable, centralized ledgers—to eliminate the need for resource-intensive consensus algorithms. Key innovations are Two-stage validation, Compliance with minimal requirements and Centralized yet secure design

Compared to national-level blockchain solutions, this approach optimizes for smaller electorates, reducing computational overhead. UML diagrams formalize the architecture, enhancing reliability, while a proof-of-concept in Oracle APEX demonstrates practicality. Limitations include reliance on centralized infrastructure, though the authors argue this simplifies implementation for academic settings. Future work may extend the framework to other domains, such as energy markets, and address quantum-resistant encryption [7].

Y. Liu et al. propose securing IoT data sharing in zero-trust environments demands solutions that balance decentralization, privacy, and fairness. Existing blockchain-based approaches, such as Fair Access and IoT Sentinel, address access control and device filtering but overlook fairness and dynamic misbehavior detection. Smart contracts have been leveraged for automation but struggle with scalability in IoT contexts. Prior works like Kim et al. (2020) and Wang et al. (2017) lack robust mechanisms to ensure participant accountability or resist collusion in adversarial settings. This paper proposes a blockchain-enabled decentralized protocol tailored for zero-trust IoT, integrating dynamic reputation system, two-phase authentication, voting-driven consensus and universal compensability security.

Key innovations include temporary symmetric keys for encrypted data exchange and a reputation chain to prioritize trustworthy participants. Compared to prior IoT blockchain solutions, this approach uniquely integrates fairness via automated penalties and reduces latency (average 0.059s per transaction in Ethereum-based tests). Proof-of-concept implementation using Ganache and Solidity demonstrates practicality, though reliance on centralized RSUs for consensus introduces scalability trade-offs. Future work aims to optimize communication overhead and quantum resistance [8].

B. A. Ahmed et al. propose existing electronic voting systems, such as Estonia‟s I-Voting and Norway‟s discontinued platform, face challenges like centralization vulnerabilities, lack of transparency, and susceptibility to cyber attacks. These systems rely on centralized servers, making them targets for DDoS attacks and state-level tampering. While cryptographic methods like blind signatures and Tor networks enhance anonymity, they fail to ensure full integrity or resist advanced threats. This paper proposes a blockchain-based e-voting system to address these gaps. Key features include Decentralization, Immutable Ledger, Anonymity & Verifiability and Conflict Resolution.

Compared to centralized systems like Estonia‟s (which allows vote overwriting), the proposed system enforces one-time voting and resists Sybil attacks by validating voters against pre-registered databases. However, limitations include reliance on secure voter devices and the inability to correct vote errors post-submission. While prior blockchain voting frameworks emphasize smart contracts or biometrics, this design prioritizes simplicity and decentralization, avoiding complex consensus mechanisms. Future work aims to address device security and introduce vote rectification mechanisms [9].

Comparative table summarizing

Criteria	**S. T. Alvi et al. [6]**	**S. V. Oprea et al. [7]**	**Y. Liu et al. [8]**	**B. A. Ahmed et al. [9]**
Technology	Blockchain, BioHash, Smart Contracts	Oracle Blockchain Tables, Encrypted Functions	Blockchain, Smart Contracts, UC Framework	Blockchain (SHA-256), Decentralized Nodes

Key Features	- Merkle trees - Miner selection - Real-time vote counting	- Two-stage validation (voting + PIN) - UML diagrams - Centralized blockchain tables	- Reputation system - Voting-driven consensus - IoT integration	- SHA-256 hashing - Longest chain rule - One-time voting
Security Mechanisms	- BioHash fingerprints - Smart contract verification	- Immutable blockchain tables - Encrypted PIN generation	- UC-secure protocol - Penalty mechanisms - Encrypted temporary keys	- Decentralized ledger - SHA-256 vote hashing
Scalability	Optimized for speed via miner selection (latency/energy metrics)	Designed for small-scale university elections	Tailored for IoT networks; efficient for distributed nodes	District-level nodes; limited by voter device security
Use Case	National/local elections	University elections	Zero-trust IoT data sharing	National/local elections
Limitations	- Device security risks - No vote changes allowed	- Centralization trade-off - No quantum resistance	- Communication overhead - Dependency on RSUs for IoT	- No vote correction - Reliance on secure voter devices
Innovations	- BioHash for biometric security - Optimized mining	Simplified architecture using blockchain tables for academia	- Reputation-driven fairness - UC framework proof	- Decentralized simplicity - Avoids smart contracts

III. RESEARCH OBJECTIVES

This research work carried out on following objectives

1. To provide a systematic voting mechanism by combining electronic voting machine (EVM) and online voting system using IoT which recognize face based on aadhar card details verification.
2. To resolve various security issues by integrating electronic voting machine with IoT devices which accepts from authentic voters and storing voting data in block chain.
3. To store voting data in election commission database and in the form of blocks to the block chain using approval of consensus algorithm, that ensure trust in transactions.
4. To provide EVM based voting system that operates based on Ethereum based blockchain as a distributed public ledger to store voting data. This approach reduces the reliance on a central authority, promoting greater trust and fairness in the voting process. To keep logs of vote transaction given by voters will be kept as anonymous with the help of Message Digest algorithm which belongs to Secure Hash Algorithm family which ensures integrity along with the transparency to voters.

IV. PROPOSED METHODOLOGY

4.1 System Architecture Overview

The system architecture leverages a decentralized blockchain framework (Ethereum), IoT devices for real-time monitoring, and biometric authentication to ensure end-to-end security. The workflow is divided into three phases:

1. **Pre-Voting Phase**:
   - **Candidate Registration**: Candidates submit documents to the Election Commission of India (ECI). A unique Candidate ID (CID) is generated using AES encryption, combining biometric facial data, Aadhaar details, and a salt value.
   - **Voter Registration**: Eligible voters are identified using Aadhaar data. Facial biometrics from the UIDAI database is processed using the Local Binary Pattern Histogram (LBPH) algorithm to train a machine learning model for real-time authentication.
2. **Voting Phase**:

- **Authentication**: Voters input their Aadhaar number, which is hashed (SHA-256) and matched against the database. Facial recognition via IoT cameras validates identity using the pre-trained LBPH model.
- **Vote Casting**: Upon successful authentication, the EVM activates. Votes are encrypted (AES-256) and stored locally in a blockchain-like structure. Simultaneously, transaction data is transmitted to an Ethereum-based blockchain via smart contracts.

3. **Post-Voting Phase**:
   - **Result Calculation**: Votes from the EVM and blockchain are decrypted (using RSA and AES private keys) and compared. Matching counts validate the election result; discrepancies trigger investigations.

4.2 Hardware Configuration

This section elaborates on the technical and procedural aspects of required to develop and deploy the system effectively also describes about hardware connectivity with blockchain using Ganache server. Set up done using tools such Raspberry Pi Pico modules. The Raspberry Pi Pico interfaces with six buttons (for candidates/NOTA), six LEDs, an LCD, and a buzzer. Raspberry Pi Pico modules integrate camera sensors of computer system using micro python coding and python module which interacts with each other using USB to TTL UART Serial Converter Module CP2102 5 Pin is a single chip USB to UART IC, as Ganache, which simulate blockchain environments for development and testing. The hardware setup ensures secure, real-time data processing and voter interaction. Key Hardware Components are as below

1. **Raspberry Pi Pico**:
   - Serves as the central control unit for the EVM.
   - Features 26 GPIO pins to interface with buttons, LEDs, LCD, and communication modules.
   - Processes voter inputs, manages encryption, and transmits data to the blockchain.
2. **IoT Devices**:
   - **Camera Module**: Captures facial images for biometric authentication. Integrated with Python-based LBPH algorithms for real-time recognition.
   - **USB-to-UART TTL Module (CP2102)**: Facilitates serial communication between the Raspberry Pi Pico and a computer for blockchain integration.
3. **Peripheral Components**:
   - **16x2 LCD Display**: Shows voter prompts and confirmation messages.
   - **LEDs and Push Buttons**: LEDs indicate candidate selection; buttons enable vote casting.
   - **Buzzer**: Provides audio feedback upon successful vote submission.

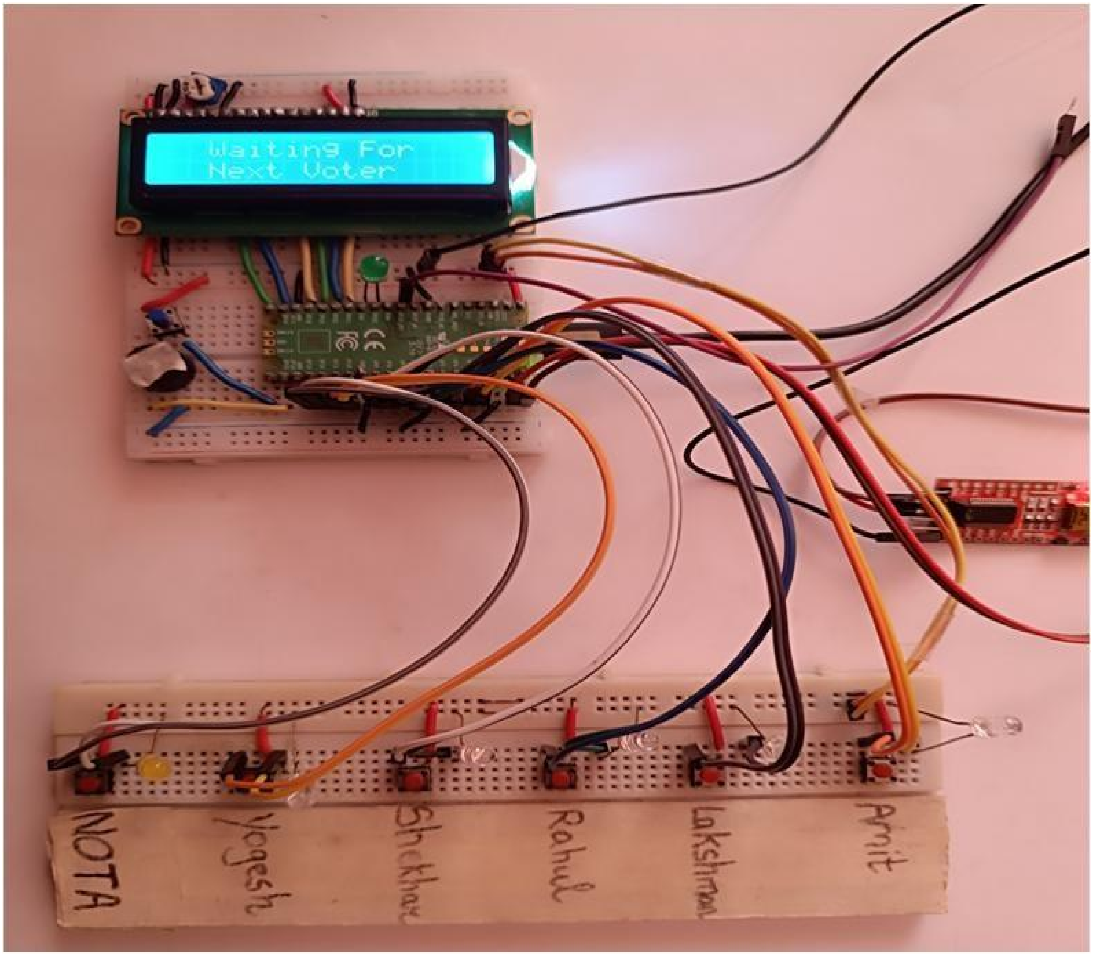

Figure 4.4: Hardware modules interconnected via Raspberry Pi Pico.

4.3 Software and Algorithms

The system employs a combination of cryptographic protocols, blockchain frameworks, and machine learning models:

1. **Blockchain Implementation**:
   - **Ethereum Network**: Hosts smart contracts written in Solidity to automate vote recording and validation.
   - **Ganache Server**: Simulates a local Ethereum blockchain for testing. Transactions are encrypted using RSA (public key) and stored as immutable blocks.
2. **Biometric Authentication**:
   - **LBPH Algorithm**: Processes facial images by dividing them into regions, extracting texture patterns, and generating histograms for comparison.
   - **Data Augmentation**: Multiple facial images (varying brightness/contrast) are used to train the model, improving recognition accuracy.

3. **Encryption Protocols**:
    - **AES-256**: Encrypts Candidate IDs and EVM vote transactions.
    - **SHA-256**: Hashes Aadhaar numbers to protect voter identity.
    - **RSA**: Secures blockchain transactions; decryption requires a private key held exclusively by the ECI.

4.4 Workflow Execution

Pre-Voting Phase:

1. **Candidate Registration**:
    - Documents are verified by the ECI.
    - A unique CID is generated using AES encryption:

      CID = AES_Encrypt(HASH(Aadhaar + Birth Year + Salt), Private_Key)
2. **Voter Registration**:
    - Aadhaar data is retrieved from the UIDAI database.
    - Facial images are augmented and processed via LBPH to train the authentication model.

Voting Phase:

1. **Authentication**:
    - Voters enter their Aadhaar number, which is hashed and matched against the database.
    - A camera captures live facial data; the LBPH model verifies identity.

2. **Vote Casting**:
    - The Raspberry Pi Pico activates the EVM upon successful authentication.
    - Votes are stored locally as encrypted blocks (AES-256) and transmitted to the Ethereum blockchain via smart contracts.

Post-Voting Phase:

1. **Result Calculation**:
    - EVM data is decrypted using AES private keys.
    - Blockchain data is decrypted using RSA private keys.
    - Results from both sources are compared; discrepancies indicate tampering.

4.5 Implementation Details

- **Smart Contracts**: Deployed on Remix IDE, the „SubmitVote‟ solidity code function records transactions on the blockchain. Each vote generates a unique transaction hash for auditability.

- **IoT Integration**: The Raspberry Pi Pico communicates with the blockchain via the CP2102 module. Real-time monitoring detects tampering attempts.
- **Edge Cases**: Invalid Aadhaar numbers or facial mismatches trigger immediate rejection, preventing unauthorized access.

V. RESULT ANALYSIS

By merging decentralized ledger technology, biometric security, and IoT-driven hardware safeguards, the proposed methodology offers a robust framework to fortify India‟s electoral infrastructure against fraud, tampering, and operational inefficiencies. The implementation and evaluation of the proposed secure electronic voting system revealed significant progress in tackling persistent challenges in voting processes. By utilizing blockchain technology, IoT devices, and Aadhaar-based biometric authentication, the system achieved substantial improvements in security, transparency, and efficiency. This section outlines the evolution of insights gained through extensive testing, performance assessments, and stakeholder feedback.

1) Security Enhancements

A key goal of this project was to ensure the highest level of security in the voting process. The blockchain network provided a tamper-resistant platform where votes were recorded as unchangeable transactions. During testing, attempts to alter recorded votes were effectively thwarted by the blockchain‟s consensus mechanism, which requires majority agreement among nodes for any changes. This decentralized approach eliminated vulnerabilities tied to traditional centralized systems, such as single points of failure and susceptibility to insider threats. Biometric authentication further bolstered security. By integrating Aadhaar-linked facial recognition, the system ensured that only authorized voters could access the voting interface.

2) Operational Efficiency

Efficiency was a critical factor assessed during pilot phases. IoT-enabled sensors streamlined the monitoring and maintenance of voting machines by providing real-time diagnostics, allowing election officials to address issues promptly. For example, during a simulated large-scale election, IoT devices identified environmental irregularities like overheating, which were resolved before disrupting the voting process. This proactive approach minimized downtime and enhanced voter confidence in the system‟s reliability.

3) Transparency and Trust

A notable achievement of the system was its ability to promote transparency. By making vote records publicly verifiable on the blockchain, the system allowed voters and independent observers to audit results without compromising voter anonymity. This openness addressed widespread concerns about electoral fraud and manipulation. IoT devices further contributed to transparency by maintaining detailed logs of all machine interactions, providing a clear audit trail for dispute resolution. For instance, during a simulated network outage, the system documented and analyzed the event, demonstrating its resilience and ability to maintain data integrity under adverse conditions.

4) Scalability and Performance

The system‟s scalability was rigorously tested to evaluate its suitability for large-scale elections. Simulations involving batches of 20, 50, 100, 1,000, and 5,000 transactions were conducted to assess blockchain throughput and latency. Results showed an average transaction processing time of 2 seconds, with minimal latency deviation even under peak loads. Additional evaluations included:

- **Stress Testing Under Peak Loads:** The system‟s ability to handle sudden surges in voter participation without compromising speed or security.
- **Network Congestion Scenarios:** Performance assessment during simulated bandwidth limitations or node failures to ensure robustness in suboptimal conditions.
- **Consistency across Scales:** Verification that transaction validation times remained stable regardless of the number of active nodes or voters.
  The findings confirmed the system‟s linear scalability, with no significant performance degradation as transaction volumes increased. This makes it a viable solution for elections ranging from small organizational polls to national-level events involving millions of participants, ensuring both speed and reliability in critical democratic processes.

5) Overall Impact

The findings highlight the transformative potential of integrating advanced technologies into electoral systems. By addressing critical issues such as security, transparency, and scalability, the proposed system establishes a new benchmark for modern democratic processes. The evolution of insights throughout the implementation and evaluation phases underscores a significant advancement in the pursuit of secure, transparent, and efficient voting mechanisms.

VI. CONCLUSION

The proposed methodology combines decentralized blockchain infrastructure, IoT-based hardware, and robust biometric authentication to address vulnerabilities in traditional voting systems. By ensuring tamper-proof vote storage, real-time monitoring, and transparent result verification, the system enhances trust and reliability in electoral processes. Future work includes optimizing computational efficiency for large-scale deployment.

References

[1] O. A. Jaisinghani, P. L. Ramteke and B.S. Dhak, (2025). Ensuring Trustworthy Elections Using IoT-Enabled Blockchain EVM Voting Mechanism with Aadhaar Card- Based Face Verification. In: Dev, A., Sharma, A., Agrawal, S.S., Rani, R. (eds) Artificial Intelligence and Speech Technology. AIST 2023. Communications in Computer and Information Science, vol 2268. Springer, Cham. https://doi.org/10.1007/978-3-031-75167-7_10

[2] O. A. Jaisinghani and P. L. Ramteke, "Evaluating the Security Impact of Face Recognition and IoT-Enabled Blockchain on Electronic Voting Machines," 2024 2nd DMIHER International Conference on Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI), Wardha, India, 2024, pp. 1-6, doi: 10.1109/ IDICAIEI61867.2024.10842869.

[3] K. M. Khan, Kashif, Arshad, Junaid and Khan, Muhammad (2018) "Secure digital voting system based on blockchain technology" International Journal of Electronic Government Research (IJEGR), 14 (1). pp. 53-62. ISSN 1548-3886.

[4] Michał Pawlak, Aneta Poniszewska-Marańda, Natalia Kryvinska, "Towards the intelligent agents for blockchain e-voting system" Procedia Computer Science, Volume 141, 2018, Pages 239-246, ISSN 1877-0509.

[5] S. Suwarjono, L. Sumaryanti, and L. Lamalewa, „„Cryptography imple- mentation for electronic voting security,"" in Proc. E3S Web Conf., vol. 328, 2021, p. 03005.

[6] S. T. Alvi, M. N. Uddin and L. Islam, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 228-233, doi: 10.1109/ICSSIT48917.2020.9214250.

[7] S. V. Oprea, A. Bâra, A. -I. Andreescu and M. P. Cristescu, "Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level," in IEEE Access, vol. 11, pp. 18461-18474, 2023, doi: 10.1109/ACCESS.2023.3247964.

[8] Y. Liu et al., "A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things," in IEEE Transactions on Computers, vol. 72, no. 2, pp. 501-512, 1 Feb. 2023, doi: 10.1109/TC.2022.3157996.

[9] B. A. Ahmed, "A Conceptual Secure Blockchain-Based Electronic Voting System" International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3,

May 2017.

[10] P. M. B. Mansingh, T. J. Titus and V. S. S. Devi, "A Secured Biometric Voting System Using RFID Linked with the Aadhar Database," 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2020, pp. 1116-1119, doi: 10.1109/ICACCS48705.2020.9074281.

[11] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

[12] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," in IEEE Software, vol. 35, no. 4, pp. 95-99, July/August 2018, doi: 10.1109/MS.2018.2801546.

[13] D. Khoury, E. F. Kfoury, A. Kassem and H. Harb, "Decentralized Voting Platform Based on Ethereum Blockchain," 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), 2018, pp. 1-6, doi: 10.1109/IMCET.2018.8603050.

[14] Sudeepthi Komatineni and Gowtham Lingala "Secured E-voting System Using Two-factor Biometric Authentication" in IEEE Xplore Part Number:CFP20K25-ART; ISBN:978-1-7281-4889-2/2020 IEEE

[15] Shubham Shinde, Manas Shende, Jeet Shah and Harshdeep Shelar "An Approach for e-Voting using Face and Fingerprint Verification" IEEE International Conference 978-1-7281-9600-8/20/2020 IEEE DOI: 10.1109, Dec -2020