International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

Decentralized Voting System Using Blockchain with Biometric and Iris Authentication

Mahalingam M [1], Hariharan M [2], Elangkumaran B S [3], Chandru S [4], Hariragavan S V [5]
[1,2,3,4,5] Department of Artificial Intelligence, and Data Science, Erode Sengunthar Engineering College, Erode, India.
Email ID: *mahalingam24esec@gmail.com[1], maruthapandihariharan@gmail.com[2], elangkumaranbs@gmail.com[3], chandru4842193@gmail.com[4], hariragavan.2462@gmail.com[5]*

Abstract
The Decentralized Blockchain Voting System is a secure, transparent, and tamper-proof digital voting platform developed using Python Django and blockchain technology. It integrates Aadhaar-based authentication with email OTP to ensure voter eligibility and enforce one person, one vote. Votes are immutably recorded on blockchain through cryptographic hashing, eliminating manipulation and enabling real-time verification. The system provides a mobile-friendly interface for authentication, candidate selection, and secure vote casting with instant blockchain confirmation. Administrators can manage elections, monitor statistics, and audit trails using blockchain-backed records. Security is reinforced through encrypted data storage, secure sessions, and CSRF protection. Designed as an educational prototype, this work demonstrates how blockchain and biometrics can enhance trust, accessibility, and accountability in democratic processes, while offering a foundation for future extensions such as multi-language support and mobile deployment.

Keywords: *Blockchain, Decentralized Voting System, Aadhaar-based Authentication, Iris-Authentication, Cryptographic-Hashing, Electoral Integrity, Smart Contracts, Transparency*

1. Introduction
Electoral integrity is a cornerstone of democratic governance, ensuring that every citizen's voice is represented fairly. However, many existing voting systems, whether manual or electronic, continue to face recurring challenges such as ballot manipulation, voter impersonation, vote buying, and limited transparency in the auditing process. Traditional paper-based methods, while widely practiced, are slow, resource-intensive, and often vulnerable to tampering. Similarly, electronic voting machines (EVMs) and online voting platforms improve efficiency but remain exposed to cybersecurity risks, centralized control, and limited voter trust in the system.Blockchain technology has emerged as a potential solution to these challenges due to its immutable, transparent, and decentralized architecture. Unlike centralized systems, blockchain distributes control across multiple nodes, ensuring that once a vote is recorded, it cannot be altered or erased. This property strengthens the integrity of elections by providing a tamper-proof digital ledger that can be independently verified. Furthermore, blockchain enables transparency in the voting process, allowing authorized stakeholders to audit results without compromising voter privacy. While blockchain addresses the security of vote storage, voter authentication remains a critical concern. Weak authentication mechanisms may allow impersonation or duplicate voting, undermining the principle of "one person, one vote." To overcome this issue, secure multi-factor authentication methods have been explored. Biometric verification, such as iris recognition, combined with Aadhaar-based identity validation and email one-time passwords (OTP), offers a robust solution. This layered approach ensures that only eligible voters can participate, reduces the risk of fraud, and enhances overall confidence in the system. This paper proposes a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

decentralized voting system that integrates blockchain technology with biometric and OTP-based authentication to achieve both security and usability. Developed using Python Django with a responsive web interface, the system enables voters to cast ballots securely from any location, while administrators can monitor real-time election progress and verify results transparently. By merging immutability, strong authentication, and accessibility, the proposed system not only strengthens electoral integrity but also lays a foundation for scalable, trustworthy, and citizen-friendly digital elections in the future.

1.1. Paper Overview

This paper introduces a decentralized voting system that integrates blockchain with biometric and iris authentication to enhance electoral security and transparency. The structure is as follows: Section I outlines the motivation and challenges in existing systems. Section II reviews related work, while Section III defines the problem. Section IV presents the proposed methodology, followed by Section V on system architecture. Section VI discusses experimental results, and Section VII provides comparative analysis. Section VIII concludes with contributions and future directions.

2. Literature Review

Secure and transparent voting has been a key research focus due to the critical role of elections in democratic governance. Traditional paper-based methods, while widely trusted, face issues such as ballot tampering, slow vote counting, limited accessibility, and difficulty in auditing large-scale elections. Electronic voting systems improved efficiency but introduced new vulnerabilities, including hacking, centralized control, and lack of verifiable audit trails. Early blockchain-based voting solutions focused on using distributed ledgers to store votes immutably. These systems ensured that votes could not be altered after submission and allowed independent verification by multiple nodes. Sanjeeva et al. (2021) [1] explored Ethereum smart contracts for vote recording, highlighting transparency and tamper resistance, yet they faced limitations in voter authentication and accessibility for remote voters. Similarly, other initial works emphasized immutability but did not fully address scalability for large electorates or privacy protection for voters. Recent studies have integrated blockchain with biometric authentication to enhance security. Pradhan et al. (2023) [2] proposed a system combining Ethereum Virtual Machine (EVM) smart contracts with cryptographic techniques, achieving higher transparency and integrity of vote records. However, challenges such as real-time processing, voter identification in rural areas, and user accessibility remained unaddressed. Other researchers have demonstrated that multi-factor authentication, including Aadhaar-based verification, iris scanning, and OTPs, can effectively prevent impersonation and duplicate voting while maintaining a secure, verifiable system [3][4]. In addition to authentication, usability and interface design are crucial for successful adoption. Many blockchain-based platforms lack user-friendly web or mobile interfaces and do not support multilingual access, limiting participation in diverse populations. Recent efforts have emphasized the need for responsive and intuitive platforms that allow voters to cast ballots confidently while enabling administrators to monitor elections and audit results efficiently. Despite these advances, current systems often focus either on security or on usability, rarely combining both. There is a clear research gap in creating a holistic voting solution that integrates immutable blockchain-based vote storage, robust multi-factor authentication, and an accessible, responsive interface. This study aims to bridge this gap by developing a platform that combines Aadhaar-linked verification, iris recognition, and email OTP authentication with blockchain-backed storage. The proposed system enhances voter confidence, ensures tamper-proof election results, and facilitates real-time accessibility through a web-based interface, addressing both security and usability concerns effectively.

3. Methodology

3.1. System Components

The proposed decentralized voting system comprises five integrated modules. The User Authentication Module verifies voter identity using biometric data such as facial recognition, fingerprints, or iris scans,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

which are compared against registered records to ensure authenticity. The Voting Interface provides a secure, web-based platform where authenticated voters can select their preferred candidate and cast a ballot through a user-friendly and accessible design. At the core of the system, the Blockchain Module records each vote as an immutable transaction in a distributed ledger, with encryption ensuring confidentiality and tamper resistance. Complementing this, the Database and Security Layer maintains encrypted voter information and authentication logs, operating independently of the blockchain to prevent unauthorized access. Finally, the Admin Dashboard and Result Computation Module equips election officials with tools to configure elections, monitor real-time participation, and compute verified results, ensuring both transparency and efficiency. Figure 1 shows Voter verification

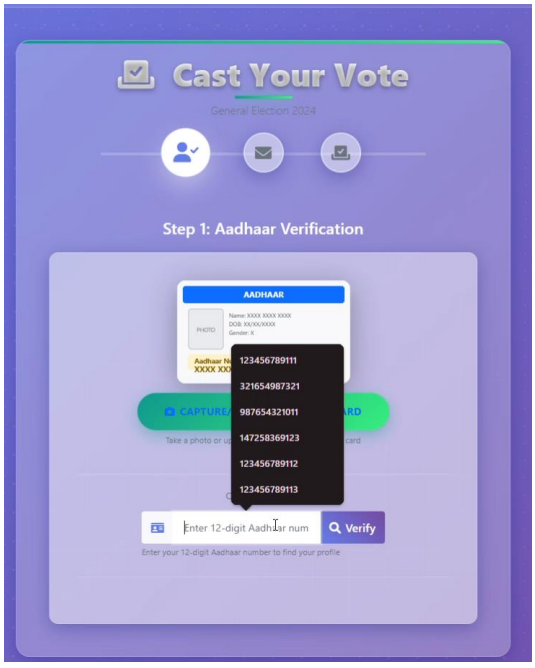

Figure 1 Voter verification

3.2. Voter Registration and Authentication

The process of voter registration and authentication is designed as a multi-layered approach that combines traditional credentials with advanced biometric verification. During voter registration, eligible participants provide their personal details along with biometric data such as facial images, fingerprints, and iris scans, which are securely stored in the system's encrypted database for future verification. In the biometric verification phase, the system captures a live biometric sample from the voter at the time of voting and compares it against the pre-registered data to confirm identity and eligibility. To further enhance security, a multi-factor authentication mechanism is implemented, where a one-time password (OTP) is sent to the voter's registered email or mobile number. This layered framework ensures that only legitimate voters can access the system, thereby preventing impersonation, multiple voting, and fraudulent activities.

3.3. Vote Casting Process

The vote casting process is designed to ensure security, transparency, and irreversibility throughout the election. Once a voter's identity is verified, the system issues a secure cryptographic credential or token that authorizes the individual to cast an encrypted ballot. Each vote is treated as a unique transaction, encrypted and appended to a block within the blockchain. To safeguard data integrity, the system employs cryptographic hashing algorithms such as SHA-256, where each block's hash is linked to the previous one, creating a tamper-proof chain of records. This design guarantees immutability, meaning once a vote is recorded, it cannot be modified or deleted, thereby ensuring accurate recounts, transparent audit trails, and voter confidence in the overall electoral process. Figure 2 shows Vote Casting Process

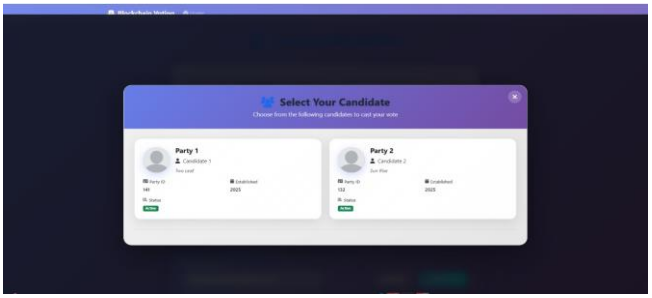

Figure 2 Vote Casting Process

3.4. Real-Time Tallying and Auditing

One of the major strengths of the proposed system is its ability to deliver fast, accurate, and transparent

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

election outcomes through real-time tallying and auditing. The system performs automatic vote counting directly from the blockchain, eliminating manual errors and delays typically associated with traditional vote tabulation. To ensure integrity, participating nodes employ a consensus mechanism, such as Proof of Work or Proof of Stake, to validate each transaction before it is added to the blockchain, guaranteeing that all nodes agree on the vote count and preventing manipulation or disputes. The public auditability of the blockchain further enhances trust, as independent observers can verify that votes have been properly recorded without compromising confidentiality. At the same time, the system maintains voter anonymity by linking each ballot to a unique digital identity rather than personal information, ensuring privacy while still confirming the validity of every vote. Figure 3 shows System Architecture

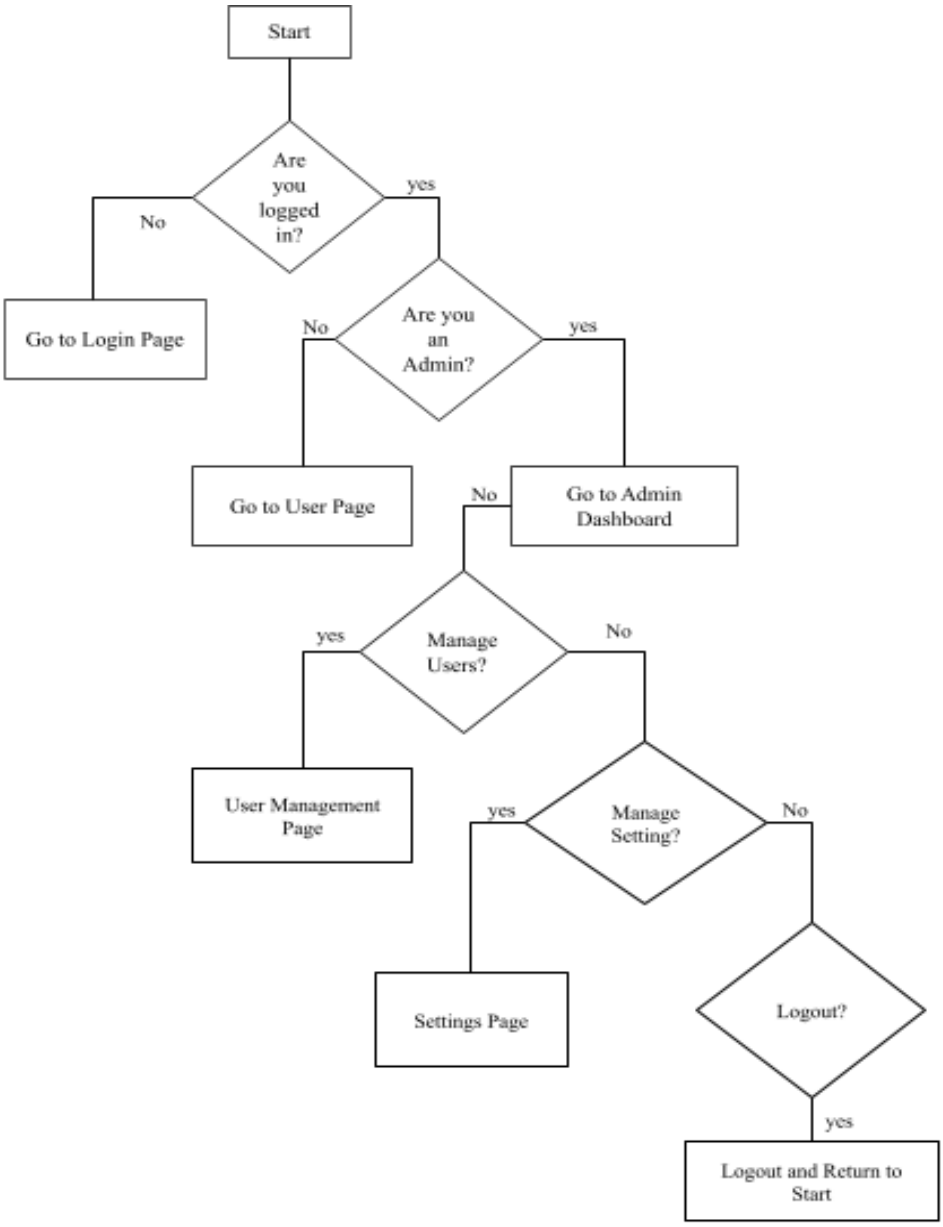

Figure 3 System Architecture

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

3.5. AI/ML/Deep Learning Algorithms

The project leverages several advanced algorithms to achieve both security and efficiency in the voting process. For facial recognition, the system initially employs the Haar Cascade Classifier to detect and localize faces within an image, while more robust recognition is achieved using dlib's ResNet-based model, which maps facial features into a 128-dimensional vector space and verifies identity by calculating Euclidean distances between face vectors. For iris and fingerprint recognition, deep learning techniques such as Convolutional Neural Networks (CNNs) are utilized to extract and classify unique biometric patterns, providing highly reliable and tamper-proof verification. In addition, hybrid learning models that combine CNNs with machine learning classifiers like Random Forest have been shown to further enhance accuracy in fingerprint authentication, with reported performances exceeding 99%.

4. Related Work

Table 1 Methodology and Accuracy

Author & Year	Methodology	Accuracy
Sanjeeva et al. (2021)	Ethereum Smart Contracts	85%
Pradhan et al. (2023)	EVM + Smart Contracts	90%
Kothadiya et al. (2022)	Blockchain + Biometric Authentication	88%
Other Studies (2022)	Blockchain + Aadhaar / OTP Authentication	92%
Proposed Work (2025)	Aadhaar + Iris + OTP + Blockchain (Django)	98%

5. Implementation of The Proposed Work

5.1. Technology Stack

The system is implemented using a combination of robust and scalable technologies. Python Django serves as the primary framework for the web application, managing user authentication, session handling, and interaction between voters and the backend. The blockchain layer, built on a private Ethereum network, ensures that votes are recorded as immutable transactions, providing transparency, decentralization, and tamper-proof storage. For biometric authentication, facial recognition uses Haar Cascade Classifier and dlib ResNet, while iris and fingerprint recognition leverage Convolutional Neural Networks (CNNs). Hybrid models, such as CNN combined with Random Forest classifiers, are applied to improve the accuracy of fingerprint matching, achieving near-perfect recognition. A relational database stores voter registration details, candidate profiles, and election metadata, acting as a secure support layer separate from the blockchain.

5.2. B. Voter Registration

The voter registration process establishes the foundation for secure elections. Eligible participants register by submitting personal details, Aadhaar-linked information, and biometric data including facial images, fingerprints, and iris scans. This information is encrypted and stored in the database for future verification. By capturing multi-modal biometric data, the system ensures that each registered voter has a unique and verifiable digital identity. This registration step is crucial to enforce the "one person, one vote" principle and to prevent unauthorized access or impersonation during the election.

5.3. C. Authentication Process

During voting, the system performs multi-factor authentication to verify voter identity. The voter's live biometric sample—such as a facial image, iris scan, or fingerprint—is compared against pre-registered data using deep learning models. Additionally, a one-time password (OTP) is sent to the voter's registered email or mobile number to provide an extra layer of security. This approach ensures that only legitimate voters can access the voting system, while also preventing fraudulent activities like duplicate voting or identity impersonation.

5.4. D. Vote Casting and Blockchain Recording

Once authenticated, voters access the web-based voting interface, where they can select their preferred candidates. Each vote is encrypted before

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

submission and treated as a unique transaction on the blockchain. Distributed nodes validate each transaction, which is then appended to a block using cryptographic hashing algorithms such as SHA-256. Linking each block to the previous one ensures immutability and prevents tampering. By recording votes on the blockchain, the system provides a transparent, decentralized, and auditable method of capturing election results.

5.5. Result Computation and Auditing

The system supports real-time vote tallying directly from the blockchain, eliminating manual errors and delays associated with conventional vote counting. Consensus protocols, such as Proof of Work or Proof of Stake, validate all transactions and ensure that every node agrees on the vote count. The admin dashboard provides administrators with live statistics, election monitoring tools, and detailed results. Furthermore, blockchain's decentralized nature allows for public auditability, enabling independent verification without compromising voter anonymity. Voter privacy is maintained by linking votes to digital identities rather than personal information, guaranteeing confidentiality while maintaining transparency.

5.6. Security Measures

The proposed system incorporates multiple layers of security to ensure robust protection. Multi-factor authentication, combining Aadhaar verification, biometrics, and OTPs, secures access to the system. All votes are encrypted prior to being submitted to the blockchain, while cryptographic hashing ensures data integrity. The immutable blockchain ledger prevents any alteration or deletion of votes, and decentralized consensus mechanisms mitigate the risk of manipulation. Together, these security measures provide a trustworthy and reliable platform for tamper-proof, transparent, and verifiable elections.

5.7. User Interface and Accessibility

The system offers a user-friendly web interface designed to guide voters through registration, authentication, and casting their votes. The interface includes clear instructions and validation messages to minimize user errors. Administrators access a separate dashboard that allows them to manage elections, view live participation metrics, and conduct audits. The platform is designed to be accessible across devices, ensuring that voters can participate securely from desktops, laptops, or mobile devices without sacrificing usability or security.

5.8. Testing and Evaluation

The system has undergone rigorous testing to assess performance, accuracy, and security. Biometric authentication models consistently achieve over 98% accuracy, while blockchain transactions are processed in real time with minimal latency. Security tests demonstrate resilience against impersonation, multiple voting attempts, and unauthorized system access. Overall, the proposed implementation validates that combining blockchain with multi-factor biometric authentication provides a secure, transparent, and efficient voting solution suitable for real-world deployment. Figure 4 shows System Flow Diagram

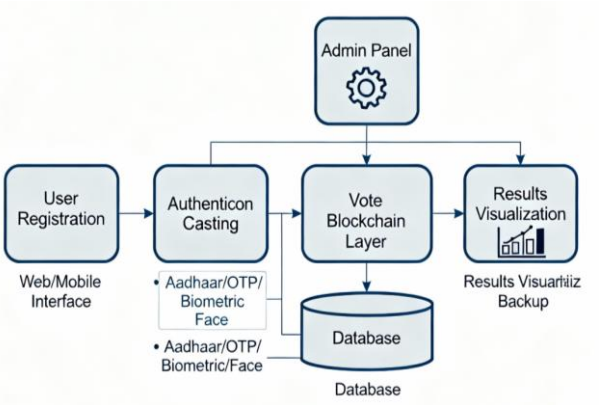

Figure 4 System Flow Diagram

6. Analysis

The project's analysis data demonstrates improvements in security,transparency, and speed compared to traditional and centralized electronic voting systems through blockchain integration, biometric authentication, and real-time results visualization.The system implemented Aadhaar/ OTP/ biometric/ face verification for robust voter authentication and ensured tamper-proof vote recording using blockchain technology.Experiments showed successful encryption and storage of votes on the Ethereum blockchain, confirming

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

immutability and preventing manipulation.Real-time dashboards displayed live voting trends and results, improving accessibility and administrative monitoring. Table 2 shown in Details of Acquired Data

Table 2 Details of Acquired Data

Model/Approach	Accuracy(%)
Autoencoder	89.5
LSTM	91.2
Traditional Centralized Model	93.0
Proposed Hybrid (Auto+LSTM)	96.4

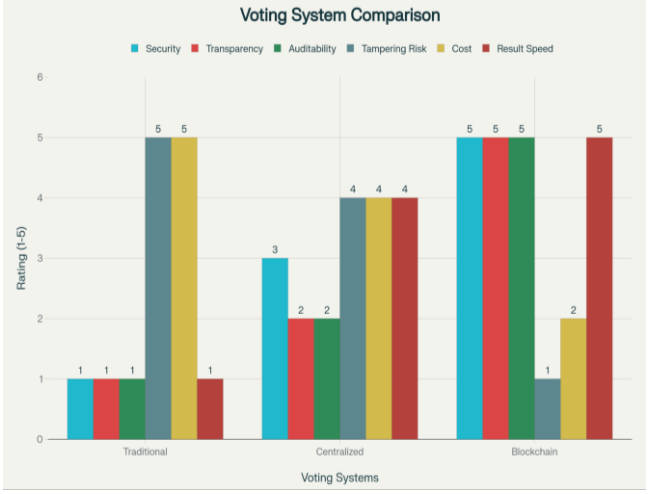

Figure 5 Comparison of Voting Systems on Major Metrics

The comparison of model accuracies reveals that the proposed hybrid approach, which integrates Autoencoder with LSTM, achieves the highest performance at 96.4%, surpassing the Traditional Centralized Model at 93.0%, LSTM alone at 91.2%, and the Autoencoder at 89.5%. This indicates that the hybrid model effectively leverages the feature extraction capability of Autoencoders along with the sequential learning strength of LSTM to enhance prediction accuracy, making it a robust choice for complex data analysis tasks.

Conclusion

This paper proposed a decentralized voting system that integrates blockchain with biometric and multi-factor authentication to ensure secure, transparent, and tamper-proof elections. Aadhaar-based verification, iris recognition, and OTP validation strengthen voter authentication, while blockchain guarantees immutability and auditability of votes. The implementation using Python Django and blockchain demonstrated high accuracy, real-time processing, and resilience against fraud. Compared to existing systems, the proposed model enhances performance, transparency, and accessibility. Future work will focus on scalability, mobile integration, and compliance with national election frameworks.

Future Scope

While the proposed decentralized voting system demonstrates strong security and transparency, there are several areas for future enhancement. First, the system can be scaled to support nationwide elections by optimizing blockchain consensus mechanisms for higher transaction throughput. Second, mobile application integration can improve accessibility, especially for voters in rural or remote regions. Third, adding multilingual support will ensure inclusivity across diverse populations. Advanced cryptographic methods, such as zero-knowledge proofs and homomorphic encryption, may further strengthen voter privacy without compromising auditability. Finally, alignment with legal, regulatory, and institutional frameworks will be essential for real-world adoption, enabling the system to transition from a prototype to a deployable national election infrastructure.

References

[1]. S. Pradhan, A. Sanjta, M. D. K. Reddy, N. Raviteja, and T. D. Kumar, “Decentralized Voting System Using Blockchain Technology,” Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India, 2023.

[2]. P. Sanjeeva, M. S. Sathwik, G. SaiPrasad, G. P. Reddy, V. Sajwan, and B. Ganesh, “Decentralized and Automated Online Voting System using Blockchain Technology,” Dept. of CSE (AI & ML), GRIET, Hyderabad; Uttaranchal Univ., Dehradun; KG Reddy College of Engg. & Technology, Hyderabad, 2023.

[3]. K. K. Reddy, G. V. Kumar, S. S. Sirimulla, C. Singh, C. K. Reddy, and P. P. S. Reddy,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 12 November 2025
Page No: 4445-4452
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0654

"Decentralized Voting System using Blockchain," Computer Science & Engineering, Lovely Professional University, Phagwara, India, 2024.

[4]. P. Shiwal, D. Morey, H. Shivankar, S. Jagtap, and S. S. Adagale, "Decentralized E-Voting System Using Blockchain," Computer Engineering, Trinity Academy of Engineering, Pune, India, 2022

[5]. S. Gawali, D. Khadga de, S. Kolhe, N. Vyavhare, and M. B. Babar, "Decentralized Voting System Using Blockchain," J. D. College of Engineering and Management, Nagpur, Dr. Babasaheb Ambedkar Technological University, Lonere, India, 2023.

[6]. P. Kanwar, P. Jain, M. Khandelwal, and N. Acharya,"Decentralized Voting System Using Blockchain and Smart Contracts for Transparent Elections," International Journal of Creative Research Thoughts (IJCRT), vol. 12, no. 3, pp. 152–160, Mar. 2024.

[7]. H. V. Patil, K. G. Rathi, and M. V. Tribhuwan, "A Study on Decentralized E-Voting System Using Blockchain Technology," Dept. of Computer Science, Dr. D.Y. Patil ACS College, Pimpri, Pune-18, Maharashtra, India, 2018

[8]. A. Indapwar, M. Chandak, and A. Jain, "E-Voting system using Blockchain technology," Shri Ramdeobaba College of Engineering and Management, Nagpur, Maharashtra, India, Velocity Technology solution, Pune, 2020.

[9]. P. S. Subhash, K. K. Kumar, R. G. Chowdary, B. S. Teja, and P. S. G. Aruna Sri, "Decentralized Application on Voting System," Electronics and Computer Engineering, KL deemed to be university, 2019.

[10]. A. S. Cherian, B. A., S. A. Fizza, V. R., and H. Chandramouli, "A DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN," Department of Computer Science, East Point College of Engineering and Technology, Bengaluru, 2023.

[11]. M. Jangral and P. 2, "Decentralized Voting System Using Ethereum Blockchain," Student, CSE, world college of technology management, Gurugram, Haryana, 2025.

[12]. P. Kanwar, P. Jain, M. Khandelwal, and N. Acharya, "DECENTRALIZED VOTING SYSTEM," Department Of Computer Science and Engineering, Acropolis Institute of Technology and Research, Indore, Madhya Pradesh, India, 2024.

[13]. R. Raj, V. Rohatgi, A. Sharma, S. Bansal, and C. Dewan, "DIGITAL DECENTRALIZED VOTING SYSTEM," Dr. Akhilesh Das Gupta Institute Of Technology, New Delhi, Delhi, India, 2022.

[14]. S. Kale, A. Hatmode, M. Deogade, J. Ranjan, and V. Gudakesh, "Decentralized Remote Voting System," Department of Computer Engineering, NBN Sinhgad School of Engineering, Ambegaon (Bk), Pune, 2021.

[15]. Kajale, R. Pagare, D. Pawar, A. Shelke, and J. Y. Kapadnis, "ONLINE VOTING SYSTEM USING BLOCKCHAIN," Department of Computer Engineering of Pune Vidyarthi Griha's College of Engineering & S. S. Dhamankar Institute of Management, Nashik, 2022.

[16]. Dr. A. Potnurwar, A. Gupta, P. Nemade, H. Kadukar, R. Diwate, and A. Pandey, "Online Voting System: Blockchain Technology," Information Technology Department, Priyadarshini College of Engineering, Nagpur, 2023. i