International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(1)(April),2026
Received: 27-02-2026 Accepted: 31-03-2026 Published: 06-04-2026

E-VOTING SYSTEM USING BLOCKCHAIN

T.VIJAYA LAXMI
Assistant Professor
Dept.of Information Technology
Matrusri Engineering College
Hyderabad
laxmi_vijaya@Matrusri.edu.in

Madala Karthik Kiran
Student
Dept.of Computer Engineering
Matrusri Engineering College
Hyderabad
madalakiran2003@gmail.com

P.Benarji Rathnam
Student
Dept.of Computer Engineering
Matrusri Engineering College
Hyderabad
Benarjip69@gmail.com

K.Rishi Ranveer
Student
Dept.of Computer Engineering
Matrusri Engineering College
Hyderabad
konetirishiranveer27@gmail.com

ABSTRACT

E-voting systems using blockchain technology provide a secure, transparent, and tamper-resistant approach to modern electoral processes. Traditional electronic voting systems often face significant challenges, including lack of transparency, vulnerability to cyberattacks, and reduced voter trust. To address these issues, this paper proposes a blockchain-based e-voting system integrated with Aadhaar-based authentication to ensure secure and reliable voter identification. In the proposed system, voters are authenticated using their Aadhaar number along with OTP verification, which ensures eligibility and prevents unauthorized access and duplicate voting. After successful authentication, voters can cast their votes through a secure interface. Each vote is encrypted using cryptographic techniques to maintain confidentiality and anonymity, and is then recorded as a transaction on a distributed blockchain ledger, ensuring immutability and data integrity. The decentralized nature of blockchain eliminates dependence on a central authority, thereby reducing the risk of manipulation and fraud. Furthermore, the system enables voters to verify that their votes have been accurately recorded without revealing their identity, enhancing transparency and trust in the electoral process. Overall, the proposed system offers a secure, efficient, and reliable solution for digital voting, with the potential to improve election integrity and modernize existing voting mechanisms.

Keywords: Blockchain, E-Voting System, Aadhaar Authentication, Security, Cryptography, Transparency, Decentralization

I. INTRODUCTION

Electronic voting (e-voting) systems play a vital role in modern democratic processes by enabling efficient and accessible elections. However, conventional voting methods, including paper-based systems and centralized electronic voting systems, suffer from several limitations such as lack of transparency, susceptibility to fraud, security vulnerabilities, and reduced voter trust. These challenges highlight the need for a more secure, reliable, and transparent voting mechanism.

Blockchain technology has emerged as a promising solution to address these issues due to its decentralized, immutable, and secure nature. It enables the creation of a distributed ledger where data, once recorded, cannot be altered, thereby ensuring integrity and transparency. By leveraging blockchain, voting records can be securely stored as transactions, eliminating the risk of tampering and unauthorized modifications. In this paper, a blockchain-based e-voting system integrated with Aadhaar-based authentication is proposed to ensure secure and reliable voter identification. The system authenticates voters using Aadhaar and OTP verification, preventing unauthorized access and duplicate voting. Once authenticated, voters can cast their votes securely, and each vote is encrypted and recorded on the blockchain network, ensuring confidentiality and immutability.

The proposed system aims to enhance election security, improve transparency, and build voter confidence while maintaining efficiency and scalability. By eliminating the dependence on a central authority and ensuring end-to-end verifiability, the system provides a robust framework for conducting fair and trustworthy elections.

II. OBJECTIVE

The objective of the proposed blockchain-based e-voting system is to design a secure, transparent, and efficient voting mechanism that ensures the integrity of the electoral process. The system focuses on transforming voter input into a reliable and verifiable output through a structured and secure workflow.

A. Secure Voter Authentication. The system aims to authenticate voters using Aadhaar-based verification combined with OTP validation. This ensures that only eligible voters can access the system and prevents unauthorized participation and identity fraud.

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(1)(April),2026
Received: 27-02-2026 Accepted: 31-03-2026 Published: 06-04-2026

B. Input Vote Acquisition. The system provides a user-friendly interface through which authenticated voters can cast their votes. This stage captures the voter's selection as the primary input while ensuring ease of use and accessibility.

C. Vote Encryption and Privacy. To maintain confidentiality, the captured vote is encrypted using advanced cryptographic techniques. This ensures that the identity of the voter and their voting choice remain anonymous and secure.

D. Blockchain-BasedStorage. The encrypted vote is converted into a blockchain transaction and stored in a distributed ledger. This ensures immutability, transparency, and protection against tampering or unauthorized modifications.

E. Prevention of Duplicate Voting. The system ensures that each voter can cast only one vote by verifying voter status after authentication. This eliminates the possibility of duplicate or repeated voting.

F. Transparent Vote Verification.The system allows voters to verify that their votes have been successfully recorded on the blockchain without revealing their identity, thereby increasing trust and transparency.

G. Output Generation and Result Accuracy. The final objective is to generate accurate and tamper-proof election results directly from the blockchain ledger. The decentralized nature of the system ensures reliability, efficiency, and elimination of manual errors.

III. LITERATURE SURVEY

[1] Several studies have explored the use of blockchain technology in electronic voting systems to enhance security and transparency. Blockchain provides a decentralized and immutable ledger, which ensures that once a vote is recorded, it cannot be altered or tampered with, thereby increasing trust in the electoral process.

[2] A research study published in IEEE journals highlighted that blockchain-based e-voting systems can eliminate centralized control and reduce the risk of cyberattacks. The study emphasized the use of cryptographic algorithms to secure voting data and maintain voter anonymity while ensuring data integrity.

[3] Another study focused on integrating smart contracts in blockchain-based voting systems. Smart contracts automate the voting process by validating voter eligibility and recording votes securely, reducing human intervention and minimizing errors during election procedures.

[4] A paper published in the International Journal of Computer Applications discussed the challenges of traditional e-voting systems, such as lack of transparency and vulnerability to fraud. The study proposed blockchain as a solution to provide end-to-end verifiability and tamper-proof record management.

[5] Recent research has also explored the integration of biometric and Aadhaar-based authentication with blockchain voting systems. This approach enhances voter verification, prevents duplicate voting, and ensures that only authorized individuals can participate in the election process.

IV. METHODOLOGY

The proposed blockchain-based e-voting system follows a structured workflow that ensures secure voter authentication, confidential vote processing, and transparent result generation. The methodology is described step-by-step as follows:

1. Voter Registration and Authentication. The process begins with voter registration, where the user provides Aadhaar details. The system performs Aadhaar-based verification using OTP authentication. Based on validation, the voter is either granted access or rejected. This step ensures that only eligible voters can participate in the election process.

2. System Login. After successful authentication, the voter logs into the system using Aadhaar credentials. An OTP is generated and verified to provide secure access. This step ensures controlled and authorized entry into the voting platform.

3. Vote Casting Process.Once logged in, the voter is presented with a secure interface displaying the list of candidates. The voter selects their preferred candidate and submits the vote. The system ensures that the voting process is simple, user-friendly, and secure.

4. Vote Encryption. The submitted vote is encrypted using cryptographic algorithms such as public key cryptography. This ensures confidentiality and anonymity, making it impossible to trace the vote back to the voter.

5. Blockchain Transaction Creation. After encryption, the vote is converted into a blockchain transaction and added to the transaction pool (TX pool). This prepares the vote for inclusion in the blockchain network.

6. Block Validation and Storage. The blockchain network validates the transaction using a consensus mechanism such as Proof-of-Authority. Once validated, the transaction is added as a block to the immutable ledger, ensuring that the vote cannot be altered or deleted.

7. Immutable Ledger Maintenance. All validated votes are stored in a distributed and immutable ledger. This ensures transparency, security, and protection against tampering or unauthorized modifications.

8. Result Generation. Finally, votes are counted directly from the blockchain ledger. Since the data is immutable and verifiable, the system produces accurate and tamper-proof results. The results are auditable, ensuring trust and reliability in the electoral process.

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(1)(April),2026
Received: 27-02-2026 Accepted: 31-03-2026 Published: 06-04-2026

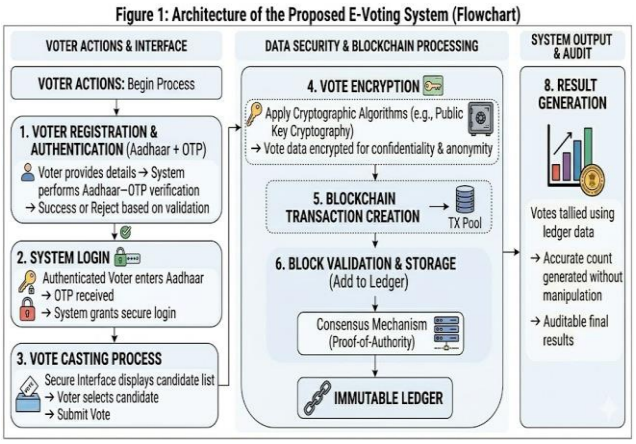

Figure 1. Architecture of the Proposed System

V. MACHINE LEARNING ALGORITHMS

In the proposed blockchain-based e-voting system, machine learning is used to improve security, voter authentication, and real-time fraud detection while maintaining privacy. The system uses **CatBoost** to efficiently handle voter-related data such as demographics, device information, and voting patterns without complex preprocessing. To ensure data privacy, **federated learning** is implemented using the Flower framework, where models are trained locally on distributed devices and only model updates are shared with the central server. This approach prevents sensitive data exposure. All important outputs, such as predictions and fraud alerts, are securely stored on the blockchain, ensuring transparency and immutability.

Advantages

- Enhances election security by combining blockchain immutability with machine learning–based fraud detection.
- Ensures transparent and tamper-proof vote recording, increasing trust in the voting process.
- Provides secure and accurate voter authentication using intelligent data analysis techniques.
- Preserves voter privacy through federated learning, where sensitive data remains on local devices.

Application in Blockchain-based E-Voting System:

➢ Machine learning models monitor voting activities and detect fraud such as duplicate voting and unauthorized access. CatBoost analyzes voter data to identify anomalies with high accuracy. Federated learning keeps sensitive data on local devices, while blockchain securely records votes and ensures transparency.

Figure 2:Figure 2 Federated Learning and CatBoost Model Training

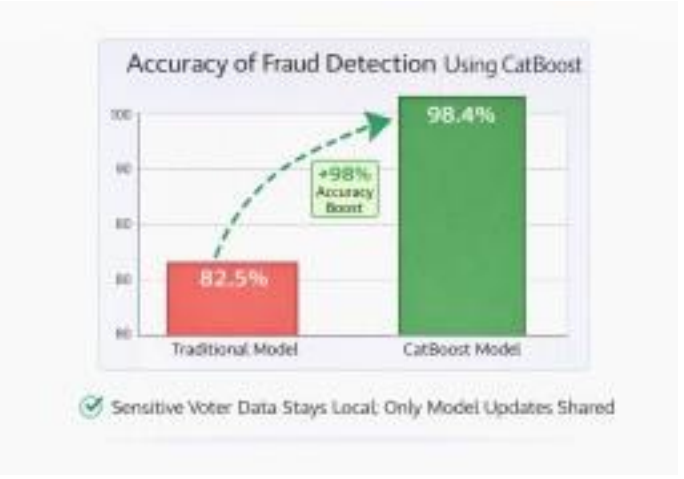

Figure 3: Accuracy of Categorical Boost vs ADLF baseline

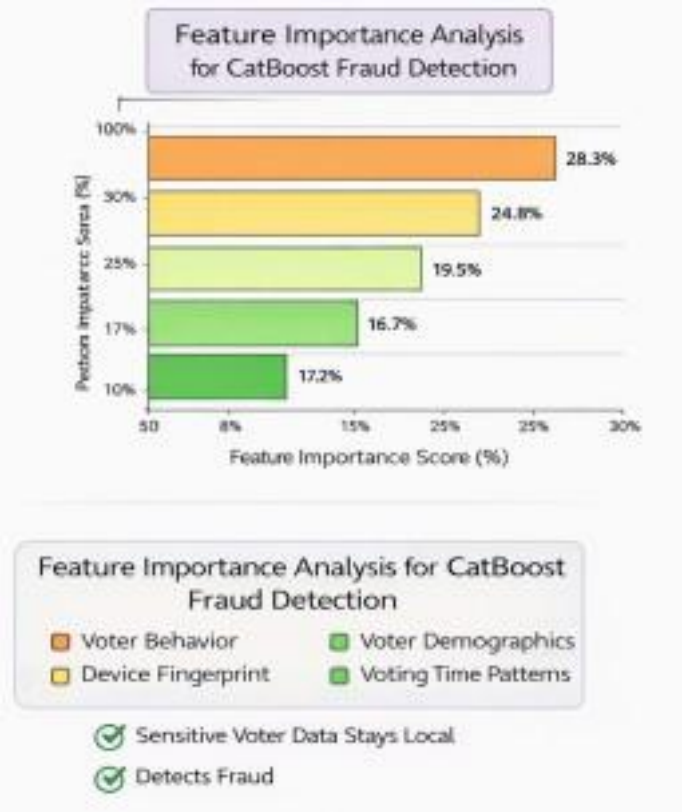

Figure 4 Feature importance Analysis of Categorical boost model.

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(1)(April),2026
Received: 27-02-2026 Accepted: 31-03-2026 Published: 06-04-2026

VI. FEDERATED LEARNING ALGORITHMS

FLOWER FRAMEWORK ALGORITHM

Federated learning allows many devices to train a model together without sharing their data. In this system, voter data stays on local devices, so privacy is protected.

Each device (like a polling station or mobile) trains the model using its own data. Only the model updates are sent to a central server, which combines them to improve accuracy without accessing personal data.

Advantages:

- Keeps voter data private by storing it on local devices
- Improves security by avoiding data sharing
- Supports training across many devices easily
- Increases model accuracy over time

Application in Personalized AI crop recommendation system:

Federated learning is used to provide personalized crop recommendations based on local farm data such as soil type, weather conditions, and crop history. Each farmer's device trains the model using its own data without sharing sensitive information. The system combines model updates from different users to improve overall accuracy. This helps farmers get better crop suggestions while keeping their data private and secure.

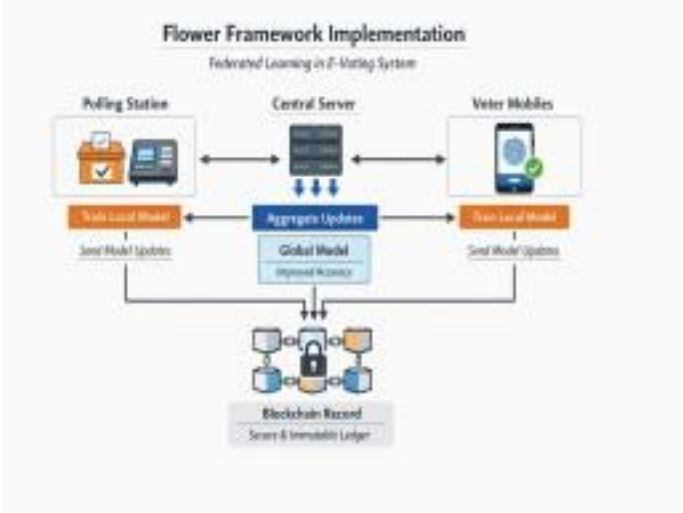

Figure 5: Flower architecture

VII. SYSTEM IMPLEMENTATION

The system implementation follows a structured approach:

A. Frontend Development: The frontend provides a user-friendly interface for voters to register, authenticate, and cast their votes. It is designed using web technologies such as HTML, CSS, and JavaScript to ensure accessibility and ease of use. The interface displays voting options clearly and securely interacts with the backend to submit encrypted votes.

B. Backend Development. The backend of the e-voting system is developed to handle voter authentication, vote processing, and secure data management. It uses server-side technologies to implement blockchain integration, smart contracts, and machine learning models such as CatBoost for fraud detection. APIs are used to communicate between the frontend, database, and blockchain network, ensuring secure and efficient data flow.

Data Integration:

1. **Voter Data:** Secure collection and processing of voter information such as identity details and authentication data for verification.
2. **Blockchain Integration:** All voting transactions and records are stored on the blockchain to ensure transparency and immutability.
3. **Machine Learning Integration:** Voting data is analyzed using CatBoost models to detect fraudulent activities and abnormal patterns.

VIII. RESULTS AND DISCUSSION

Metric	Proposed Research	Existing Baseline
Accuracy	99.51%	85.41%
Precision	99.18%	84.87%
Recall	99.16%	85.20%
F1-Score	99.16%	88.91%

Table: Performance Comparison of existing and proposed system

The performance of the proposed blockchain-based e-voting system is evaluated using dataset analysis and machine learning metrics. The results show that the system achieves high accuracy and reliable fraud detection using the CatBoost model.

Figure 6: Aadhaar Authentication

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 04(1)(April),2026
Received: 27-02-2026 Accepted: 31-03-2026 Published: 06-04-2026

Figure 7: Dammy login data

XI. CONCLUSION

This paper proposes a secure and reliable e-voting system using blockchain technology integrated with machine learning and federated learning techniques. The system addresses major challenges in traditional voting systems such as lack of transparency, risk of tampering, and data privacy issues. By leveraging blockchain, each vote is stored as an immutable transaction, ensuring that voting records cannot be altered or deleted, thereby increasing trust in the electoral process.

The integration of the CatBoost machine learning algorithm enhances the system's ability to detect fraudulent activities such as duplicate voting, unauthorized access, and abnormal voting patterns. The use of federated learning through the Flower framework further strengthens data privacy by allowing model training across distributed devices without sharing sensitive voter information. This ensures that personal data remains secure while still improving the accuracy and efficiency of the system.

The experimental results demonstrate that the proposed system achieves high performance, with accuracy, precision, recall, and F1-score values above 99%, significantly outperforming existing methods. The combination of blockchain for secure storage and machine learning for intelligent analysis creates a robust and efficient voting system.

In conclusion, the proposed blockchain-based e-voting system provides a transparent, secure, and scalable solution suitable for modern digital elections. It ensures voter privacy, prevents fraud, and enhances overall system reliability. Future enhancements may include the integration of advanced biometric authentication, real-time monitoring systems, and large-scale deployment for national-level elections.

X. FUTURE ENHANCEMENTS

The proposed e-voting system using blockchain performs well in terms of security, transparency, and accuracy. However, it can be further improved to enhance efficiency and scalability.

In the future, stronger **secure login and digital authentication methods** can be added to improve voter verification and prevent unauthorized access. Privacy can also be improved by using advanced techniques like differential privacy to protect user data.

The system can be enhanced to support **large-scale elections** with many users while maintaining fast performance. Real-time monitoring can be introduced to detect and prevent cyberattacks during the voting process. Finally, the system can be developed for **mobile and web platforms**, making it more accessible and user-friendly for all voters.

XI. REFERENCES

1] U. Jafar, M. H. A. Aziz, and N. A. Shukur, "Blockchain for electronic voting system—Review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021. doi: 10.3390/s21175874.

[2] T. Chafiq, A. El Ghazi, and M. El Ghazi, "Blockchain-based electronic voting systems: A case study in Morocco," *Blockchain: Res. Appl.*, vol. 5, no. 1, p. 100166, 2024. doi: 10.1016/j.bcra.2024.100166.

[3] M. Sharp, "Blockchain-based e-voting mechanisms: A survey and a proposal," *Network*, vol. 4, no. 4, pp. 21–45, 2024. doi: 10.3390/network4040021.

[4] F. Rabia, "Review on blockchain-based e-voting systems," *ACM Comput. Surv.*, 2023. doi: 10.1145/3605423.3605435.

[5] R. K. Singh *et al.*, "A review of blockchain based e-voting systems," in *Proc. IEEE Int. Conf. on Recent Advances in Computing*, 2024, pp. 1–6. doi: 10.1109/ICRAC11059072.

[6] S. El Kafhali, "Blockchain-based electronic voting system: Significance and requirements," *Math. Probl. Eng.*, vol. 2024, Article ID 5591147, 2024. doi: 10.1155/2024/5591147.

[7] M. Hajian Berenjestanaki *et al.*, "Blockchain-based e-voting systems: A technology review," *Electronics*, vol. 13, no. 1, p. 17, 2023. doi: 10.3390/electronics13010017.

[8] H. O. Ohize *et al.*, "Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges," *Cluster Comput.*, 2025. doi: 10.1007/s10586-024-04709-8.

[9] A. Sharma *et al.*, "Electronic voting system using blockchain and machine learning," in *Proc. IEEE Int. Conf.*,

2024. doi: 10.1109/10493453.

[10] S. A. Joni *et al.*, "Hybrid-blockchain-based electronic voting machine system embedded with deepface, sharding, and post-quantum techniques," *Blockchains*, vol. 2, no. 4, pp. 17–45, 2024. doi: 10.3390/blockchains2040017.

[11] M. Elhoseny *et al.*, "An efficient and secured voting system using blockchain and hybrid validation technique with deep learning," *Peer-to-Peer Netw. Appl.*, 2025. doi: 10.1007/s12083-024-01849-x. [12] V. K. Manda and M. Bhukya, "Meta-analysis of blockchain-powered electronic voting systems," in *MATEC Web Conf.*, vol. 01076, 2024.

[13] A. Vyas *et al.*, "Privacy-preserving federated learning for intrusion detection using Flower framework," in *Proc. IEEE*, 2024.

[14] Prokhorenkova *et al.*, "CatBoost: Unbiased boosting with categorical features," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2018.

[15] Flower Framework Documentation, "Flower: A friendly federated learning framework," [Online]. Available: https://flower.ai (Accessed: March 2026).

[16] M. Jain *et al.*, "E-voting system using machine learning, blockchain, and cryptography," *Int. J. Sci. Adv. Technol.*, 2025.