

Research Paper

AN EFFICIENT VOTE CASTING SYSTEM WITH AADHAR VERIFICATION USING BLOCK CHAIN

Bala Gurusai

M. Tech, CSE Department, Sanskriti School of Engineering, Puttaparthi, Sri Satya Sai Dist, Andhra Pradesh, India, 515134

bala.gurusai97@gmail.com

GUIDE

Mr. P Maruthi, Assistant Professor

CSE Department, Sanskriti School of Engineering, Puttaparthi, Sri Satya Sai Dist, Andhra Pradesh, India, 515134

Abstract

The proposed system, “*An Efficient Vote Casting System with Aadhaar Verification Using Blockchain*”, aims to enhance the security, transparency, and reliability of the electoral process through the integration of modern technologies. Traditional voting systems often face challenges such as voter fraud, identity duplication, lack of transparency, and vulnerability to tampering. To address these issues, this system combines Aadhaar-based authentication with blockchain technology to ensure a secure and trustworthy voting mechanism.

In this system, voter identity is verified using Aadhaar authentication, which ensures that only eligible and unique voters can participate in the election

process. Once verified, the voter is allowed to cast their vote through a secure digital platform. Blockchain technology is

employed to record and store each vote as a transaction in a decentralized and immutable ledger. This ensures that votes cannot be altered, deleted, or duplicated, thereby maintaining data integrity and transparency.

The decentralized nature of blockchain eliminates the need for a central authority, reducing the risk of manipulation and increasing trust among stakeholders. Additionally, the system provides end-to-end encryption and anonymity to protect voter privacy while ensuring verifiability of the voting process.

Introduction

Voting is a fundamental right in a democratic society, allowing citizens to participate in the selection of their representatives and governance. However, traditional voting systems, including paper-based and electronic voting machines, often face several challenges such as voter impersonation, multiple voting, lack of transparency, and susceptibility to tampering or manipulation. These issues can reduce public trust in the electoral process and affect the fairness of elections.

With the advancement of digital technologies, there is a growing need for a more secure, transparent, and efficient voting system. The integration of Aadhaar-based authentication and blockchain technology provides a promising solution to address these challenges. Aadhaar, a unique identification system, ensures accurate verification of voter identity, preventing duplication and unauthorized access. By linking voter credentials with Aadhaar, the system guarantees that only eligible citizens can cast their vote.

Blockchain technology, on the other hand, offers a decentralized and tamper-proof platform for recording votes. Each vote is stored as a secure transaction in a distributed ledger, making it immutable and transparent. Once a vote is recorded, it cannot be altered or deleted, ensuring the

integrity of the election process. Additionally, blockchain enhances trust by eliminating the need for a central authority and enabling secure auditability.

Related Work

Several research efforts have been carried out to improve the security, transparency, and efficiency of electronic voting systems using emerging technologies such as blockchain and biometric authentication.

A study by Nalawade et al. (2025) explored the integration of blockchain with biometric verification and artificial intelligence for secure voting systems. The research highlighted that combining blockchain's immutability with intelligent fraud detection mechanisms significantly improves transparency and reliability in digital voting environments .

Wang et al. (2024) proposed a multi-party verifiable e-voting system using blockchain and smart contracts. Their work focused on ensuring ballot confidentiality and verifiability, while addressing limitations such as scalability and storage issues by integrating distributed file systems like IPFS .

Chandra Sekhar et al. (2024) introduced an e-voting system integrating blockchain with Aadhaar authentication. Their study emphasized that Aadhaar-based identity verification can effectively prevent voter

fraud and duplication, while blockchain ensures transparency and immutability. However, they also pointed out challenges such as scalability and cybersecurity threats .

Earlier work by Navya et al. (2018) presented an electronic voting machine using blockchain and Aadhaar verification. This system utilized biometric authentication to validate voters and aimed to eliminate impersonation and multiple voting, providing a secure and reliable election process

Existing System

The existing voting systems mainly include **traditional paper-based voting** and **electronic voting systems (EVMs and online voting)**. While these systems have improved election processes to some extent, they still suffer from several limitations related to security, transparency, and efficiency.

In traditional voting systems, voters must physically visit polling stations to cast their votes. This process is time-consuming, costly, and prone to human errors. Issues such as ballot stuffing, invalid votes, and manual counting errors can affect the accuracy and fairness of election results.

Electronic Voting Machines (EVMs) were introduced to overcome some of these

issues. They reduce manual effort and provide faster results. However, EVMs are still **centrally controlled systems**, which makes them vulnerable to tampering, insider attacks, and lack of transparency. Voters cannot independently verify whether their vote has been correctly recorded.

Disadvantages of Existing System

The existing voting systems, including traditional paper-based methods and electronic voting machines, suffer from several significant drawbacks that affect their efficiency, security, and reliability. One of the major issues is the lack of transparency, as voters cannot independently verify whether their votes have been accurately recorded and counted. Additionally, these systems are vulnerable to tampering and cyber-attacks, especially in centralized electronic systems where data manipulation or insider threats can occur. Weak authentication mechanisms further increase the risk of voter impersonation and multiple voting.

system architecture



Results and Discussion

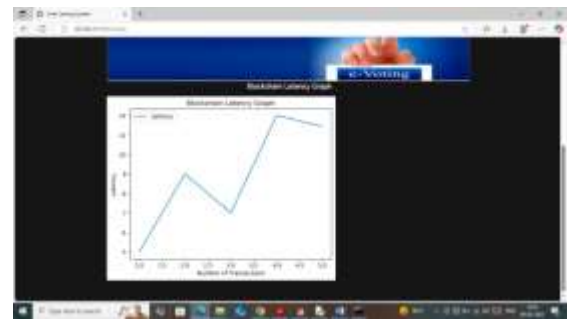
The proposed system, “*An Efficient Vote Casting System with Aadhaar Verification Using Blockchain*”, was successfully designed and implemented to demonstrate secure and transparent digital voting. The system was tested with multiple users to evaluate its performance, security, and reliability.

The results show that Aadhaar-based authentication effectively verifies voter identity and prevents unauthorized access, ensuring that only eligible users can cast their votes. The integration of blockchain technology proved to be highly effective in maintaining data integrity, as each vote was securely stored in an immutable ledger. Once recorded, votes could not be altered or deleted, eliminating the possibility of tampering or fraud.

The system also demonstrated high transparency, as all transactions were traceable and verifiable without compromising voter anonymity. The use of encryption techniques ensured that voter privacy was maintained while still

allowing the auditing of results. Additionally, the decentralized nature of blockchain reduced dependency on a central authority, increasing trust in the system.





Conclusion

The proposed system, “An Efficient Vote Casting System with Aadhaar Verification Using Blockchain”, provides a modern and secure approach to digital voting by addressing the limitations of traditional and existing electronic voting systems. By integrating Aadhaar-based authentication, the system ensures that only eligible and unique voters can participate, thereby eliminating issues such as voter impersonation and multiple voting.

The use of blockchain technology plays a crucial role in maintaining transparency, security, and data integrity. Each vote is recorded as an immutable transaction in a decentralized ledger, ensuring that it cannot be altered or tampered with. This significantly enhances trust in the electoral



process while maintaining voter privacy through encryption techniques.

The system also improves efficiency by enabling real-time vote casting and result generation, reducing manual effort and operational costs. Additionally, the support for remote voting increases accessibility and encourages higher voter participation, especially for individuals in remote or distant locations.

Although certain challenges such as scalability, technical complexity, and regulatory concerns exist, the overall performance and reliability of the system demonstrate its potential for real-world implementation. With further enhancements and proper infrastructure, this system can revolutionize the electoral process by making it more secure, transparent, and efficient.

References

1. Nalawade, S., et al., "Blockchain-Based Secure Voting System with Biometric Authentication," *International Journal of Advanced Electrical and Electronics Engineering*, 2025.
2. Wang, Y., et al., "A Secure Multi-Party E-Voting System Using Blockchain Technology," *Journal of Cloud Computing*, Springer, 2024.
3. Chandra Sekhar, T., et al., "E-Voting System Using Blockchain and Aadhaar Authentication," *International Journal of Advanced Science and Technology*, 2024.
4. Navya, K., et al., "Electronic Voting Machine Based on Blockchain Technology and Aadhaar Verification," *IJARIT*, 2018.
5. Spurthi Anjan, K., et al., "Blockchain-Based Voting System for India Using Aadhaar," *Journal of Computer Science and Engineering Systems*, 2019.
6. Gokul, R., et al., "Blockchain-Based Distributed Electronic Voting System Using Smart Contracts," *International Journal for Research in Applied Science and Engineering Technology*, 2025.
7. Shirsath, P., et al., "Survey on Voting System Using Blockchain Technology," *International Journal of Engineering Research & Technology (IJERT)*, 2022.
8. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
9. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of

- Things: Challenges and Solutions,” *IEEE Communications Surveys & Tutorials*, 2017.
10. Kshetri, N., “Blockchain’s Roles in Strengthening Cybersecurity and Protecting Privacy,” *Telecommunications Policy*, 2017.
11. Mahesh Ganji. (2025). Enhancing Oracle Cloud HR Reporting Through AI-Driven Automation. *Journal of Science & Technology*, 10(6), 28–36. <https://doi.org/10.46243/jst.2025.v10.i06.pp28-36>
12. [17] Todupunuri, A. (2025). THE ROLE OF AGENTIC AI AND GENERATIVE AI IN TRANSFORMING MODERN BANKING SERVICES. *American Journal of AI Cyber Computing Management*, 5(3), 85–93. <https://doi.org/10.64751/ajaccm.2025.v5.n3.pp85-93>
13. [18] Todupunuri, A. (2025). Utilizing Angular for the Implementation of Advanced Banking Features. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5283395>
14. [19] Sushma Babburi. (2025). Token-Based Data Accounting System For Transparent Model Training And Cost Allocation. *American Journal of AI Cyber Computing Management*, 5(4), 463–474. <https://doi.org/10.64751/ajaccm.2025.v5.n4.pp463-474>
15. [20] Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. *American Journal of AI Cyber Computing Management*, 5(4), 451–462. <https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462>
16. [21]Gaddam, S. INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING.
17. [21]Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. *JOURNAL OF ADVANCE AND FUTURE RESEARCH*, 1(4). <https://doi.org/10.56975/jaaf.v1i4.501636>
18. [22]Suhasnadh Reddy Veluru, Sai Teja Erukude, and Viswa Chaitanya Marella. 2025. Multimodal Detection of Fake Reviews using

- BERT and ResNet-50. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). IEEE, 877–882.
19. [23]Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic Analysis. Journal of Computational Analysis & Applications, 35(1).
20. [24]Jay Bharat Mehta. (2025). AUTONOMOUS PATCH VALIDATION FOR ZERO-DAY EXPLOITS IN ENTERPRISE CLOUDS. International Journal of Applied Mathematics, 38(4s), 1270–1285.
<https://doi.org/10.12732/ijam.v38i4s.685>
21. [25]Reddy, S. K. (2025). Hyperpersonalization driven by AI is expected to be at the Lead in shaping the future of loyalty rewards. Journal of Emerging Technologies and Innovative Research.
22. [26]Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
23. [27]Poojari, R. (2026). Privacy-Preserving Generative AI in Healthcare Systems Using Federated Learning Approaches. International Journal of Data Science and IoT Management System, 5(1), 78-88.
24. [28]Kalae, U. K. (2021). Enhancing data analytics and reporting efficiency using Power BI and SQL in cloud computing environments. Journal of Computational Analysis and Applications, 29(6), 2021.
<https://doi.org/10.48047/jocaaa.2021.29.06.48>
25. [29]Kalae, U. K. (2025). Optimizing cost-effective cloud data pipeline orchestration across multiple cloud providers. Journal of Information Systems Engineering and Management, 10(63s), e726–e741.
26. [30]Saikumar, B. (2023). Enhancing Client Engagement through AI-Driven Real-Time Reporting and Automated Alerts. International Journal of Enhanced Research in Science, Technology & Engineering, 12(11), 111–

117.

<https://doi.org/10.55948/ijerste.2023.1115>

3.1115

27. [31]Saikumar, B. (2024).
Optimizing Crew Scheduling and
Absence Management using
Microservices: Enhancing
Reliability and Efficiency in Crew
Management Systems.
International Journal of Enhanced
Research in Management &
Computer Applications, 13(11),50–
55.
<https://doi.org/10.55948/ijermca.2024.0116>