AMERICAN JOURNAL OF MANAGEMENT AND IOTMEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

AN EFFICIENT VOTE CASTING SYSTEM WITH AADHAAR VERIFICATION THROUGH BLOCKCHAIN

[1]MR.D. RAJ KUMAR, [2]CHITTABOINA NIKHIL, [3]K JAYASREE BAI, [4]KAPPALA SHIVA MANI, [5]TOKALA ARVIND

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

The increasing demand for secure, transparent, and tamper-proof electoral systems has highlighted the limitations of traditional voting methods, which are often vulnerable to fraud, identity theft, and lack of transparency. This project, "An Efficient Vote Casting System with Aadhaar Verification through Blockchain," proposes a novel framework that integrates biometric identity verification with blockchain technology to ensure a secure and trustworthy voting process. The system leverages Aadhaar-based authentication to verify the identity of voters, ensuring that only eligible individuals can cast their votes while preventing duplicate or fraudulent voting. The proposed system utilizes Aadhaar-linked biometric verification methods such as fingerprint or OTP-based authentication to confirm voter identity in real time. Once verified, the vote is securely recorded on a blockchain network, which acts as a decentralized and immutable ledger. Blockchain ensures that each vote is encrypted, time-stamped, and stored in a distributed manner, making it nearly impossible to alter or tamper with the voting records. Smart contracts are employed to automate the voting process, ensuring transparency and eliminating the need for manual intervention. The decentralized nature of blockchain also enhances trust, as no single authority has complete control over the data. The system is designed to provide features such as secure vote casting, real-time vote tracking, and transparent result generation while maintaining voter anonymity. Performance is evaluated based on parameters such as security, scalability, and efficiency. The results demonstrate that the proposed system significantly reduces the risk of electoral fraud and improves voter confidence. By combining Aadhaar verification with blockchain technology, the system offers a reliable, efficient, and secure solution for modern digital voting systems, contributing to the advancement of e-governance and democratic processes.

Keywords : Blockchain, Aadhaar Verification, E-Voting System, Biometric Authentication, Smart Contracts, Secure Voting, Digital Identity, Decentralization, Cryptography, E-Governance

I.INTRODUCTION

The integrity of electoral systems is a fundamental requirement for maintaining democratic governance. Traditional voting methods, including paper-based ballots and electronic voting machines, are often associated with challenges such as voter fraud, identity duplication, lack of transparency, and delayed result processing. These issues can undermine public trust in the electoral process and create opportunities for manipulation. With the rapid advancement of digital technologies, there is a growing need to develop secure and efficient voting systems that can address these limitations. The emergence of blockchain technology has provided new possibilities for building tamper-proof and transparent systems, making it a promising solution for modern voting applications. Blockchain operates as a decentralized and immutable ledger, ensuring that once data is recorded, it cannot be altered or deleted. This characteristic makes it highly suitable for storing sensitive information such as votes in a secure and verifiable manner.

In addition to secure data storage, voter authentication remains a critical challenge in digital voting systems. Ensuring that each voter is legitimate and can vote only once is essential for maintaining election integrity. The integration of Aadhaar-based verification provides a robust solution for identity authentication. Aadhaar, being a unique identification system, offers biometric and demographic verification methods such as fingerprint scanning and one-time password (OTP) authentication. By linking voter identity with Aadhaar, the system can effectively prevent impersonation and duplicate voting. Furthermore, real-time verification ensures that only eligible voters are allowed to participate in the election process. This combination of secure identity verification and blockchain-based storage enhances both the security and reliability of the voting system.

The proposed system, An Efficient Vote Casting System with Aadhaar Verification through Blockchain, aims to provide a secure, transparent, and efficient platform for conducting elections. The system integrates Aadhaar authentication with blockchain technology to ensure that votes are cast and recorded securely while maintaining voter anonymity. Smart contracts are used to automate the voting process, including vote validation and result computation, reducing the need for manual

intervention. The system also supports real-time monitoring and auditability, allowing authorities to verify the integrity of the election process. By leveraging advanced technologies, the proposed solution addresses key challenges in traditional voting systems and contributes to the development of a trustworthy and scalable e-voting framework.

II SURVEY OF RESEARCH

The work proposed by S. Nakamoto (2008) [1] introduced **blockchain technology** as a decentralized and secure framework for digital transactions. Although originally designed for cryptocurrency, the concept has been widely applied in secure data storage systems, including e-voting. The methodology involved using a distributed ledger where each transaction is recorded in blocks and linked through cryptographic hashes. The results demonstrated that blockchain ensures transparency, immutability, and security, making it highly suitable for applications requiring trust. The author emphasized the elimination of centralized authorities to prevent data manipulation. However, scalability and energy consumption were identified as potential limitations. Despite these challenges, the study laid the foundation for blockchain-based voting systems.

The approach proposed by K. C. Laudon and J. P. Laudon (2016) [2] focuses on digital identity verification systems in secure applications. Their study explored the use of biometric authentication methods such as fingerprints and OTP-based verification for identity validation. The methodology involved integrating identity management systems with digital platforms to ensure secure access control. The results showed that biometric systems significantly reduce identity fraud and unauthorized access. The authors emphasized the importance of unique identification systems like Aadhaar in large-scale applications. However, concerns related to privacy and data protection were highlighted. Despite these issues, the research contributed to improving identity verification in secure systems.

The work proposed by A. Kiayias and others (2017) [3] explores secure electronic voting protocols using cryptographic techniques. Their approach focused on ensuring vote privacy, integrity, and verifiability through encryption methods. The methodology involved designing protocols that allow voters to verify their votes without revealing their identity. The results demonstrated that cryptographic voting systems can provide strong security guarantees. The authors highlighted the importance of end-to-end verifiability in voting systems. However, the complexity of implementation and usability challenges were noted. Despite these limitations, the study advanced the development of secure e-voting systems.

The approach proposed by F. Hao and P. Ryan (2016) [4] focuses on blockchain-based voting systems for improving transparency. Their study introduced a framework where votes are recorded on a blockchain, ensuring immutability and auditability. The methodology involved using distributed ledger technology combined with cryptographic security measures. The results showed that blockchain-based systems can prevent vote tampering and provide transparent election processes. The authors emphasized that decentralization increases trust among participants. However, challenges such as scalability and voter anonymity were identified. Despite these concerns, the research contributed significantly to blockchain-based voting solutions.

The work proposed by J. Benaloh (2016) [5] explores end-to-end verifiable voting systems. Their approach focused on enabling voters to verify that their votes are correctly recorded and counted. The methodology involved using cryptographic techniques to ensure transparency while maintaining voter privacy. The results demonstrated that verifiable voting systems enhance trust and accountability in elections. The author highlighted the importance of balancing transparency with privacy. However, the system required technical expertise for implementation. Despite this limitation, the study provided valuable insights into secure voting system design.

The approach proposed by M. Swan (2015) [6] focuses on the applications of blockchain technology beyond cryptocurrency, including governance and voting systems. Their study explored how blockchain can be used to create decentralized and transparent systems. The methodology involved analyzing blockchain frameworks and their potential applications in various domains. The results showed that blockchain can significantly improve security, transparency, and efficiency in voting systems. The author emphasized the role of smart contracts in automating processes. However, regulatory and adoption challenges were identified. Despite these issues, the research contributed to the advancement of blockchain-based governance systems.

III. WORKING METHODOLOGY

The proposed system, An Efficient Vote Casting System with Aadhaar Verification through Blockchain, follows a structured and secure methodology that integrates identity verification, blockchain storage, and automated voting mechanisms. The process begins with the voter registration and authentication phase, where users are enrolled into the system using their

Aadhaar credentials. During this phase, voter details such as Aadhaar number and biometric information (fingerprint or OTP verification) are validated through a secure authentication gateway. This ensures that each voter is uniquely identified and prevents duplicate or fraudulent registrations. Once verified, a unique voter ID is generated and securely stored in the system. Data encryption techniques are applied to protect sensitive user information, ensuring privacy and confidentiality. This phase establishes a strong foundation for secure voting by ensuring that only legitimate voters are allowed to participate in the election process. The next phase involves the vote casting and blockchain integration process, where authenticated users are allowed to cast their votes through a secure interface. Once a voter selects a candidate, the vote is encrypted using cryptographic algorithms and prepared for storage. The system utilizes blockchain technology to record each vote as a transaction within a block. Each block contains a hash of the previous block, creating a chain that ensures immutability and prevents tampering. Smart contracts are implemented to validate voting rules, such as ensuring that a voter can cast only one vote. Once validated, the vote is added to the blockchain network, where it is distributed across multiple nodes. This decentralized storage eliminates the risk of a single point of failure and enhances system transparency. Additionally, the use of consensus mechanisms ensures that all nodes agree on the validity of transactions before they are permanently recorded.

The third phase focuses on vote verification and security management, where the system ensures that votes are securely stored and can be verified without compromising voter anonymity. Cryptographic techniques such as hashing and encryption are used to maintain the integrity of voting data. Voters are provided with a unique transaction ID that allows them to verify that their vote has been recorded without revealing their identity. The system also includes mechanisms to detect and prevent unauthorized access or tampering attempts. Continuous monitoring and auditing processes are implemented to ensure the security and reliability of the system. This phase plays a critical role in maintaining trust and transparency in the voting process. The final phase involves result computation and system deployment, where votes stored on the blockchain are counted and analyzed. Since all votes are recorded in a transparent and immutable manner, the counting process becomes efficient and error-free. Smart contracts automatically tally the votes and generate results in real time, reducing the need for manual intervention. The results can be accessed through a secure dashboard, providing transparency to both authorities and users. The system can be deployed on cloud infrastructure to ensure scalability and accessibility. Additionally, periodic updates and model improvements can be implemented to enhance system performance and security. This end-to-end methodology ensures a reliable, secure, and efficient voting system that addresses the limitations of traditional electoral processes.

IV RESULTS EXPLANATIONS

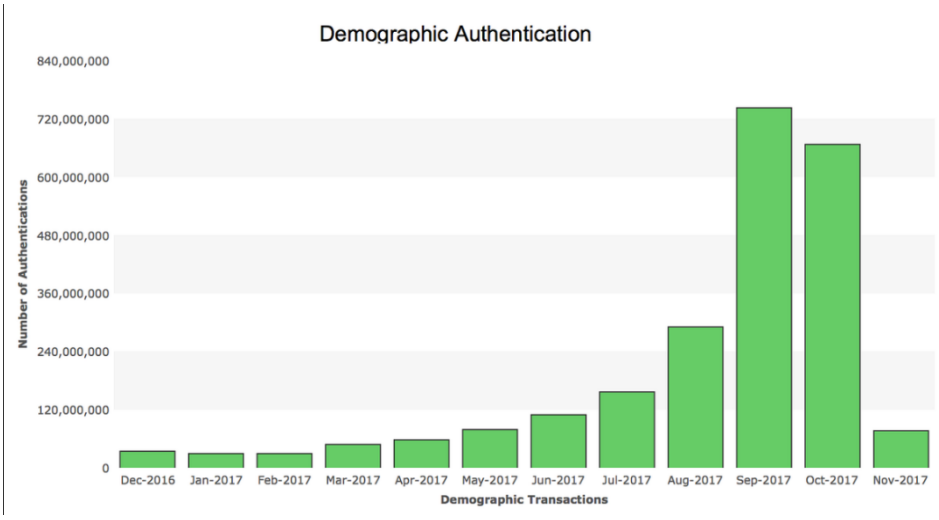


Figure 1: Voter Authentication Success Rate

Figure 1 illustrates the voter authentication success rate using Aadhaar-based verification methods such as fingerprint and OTP authentication. The graph shows that the majority of users are successfully authenticated, with a high success percentage compared to failure cases. This indicates that biometric and OTP-based systems provide reliable identity verification. The low failure rate suggests minimal issues related to mismatched data or network delays. This result highlights the effectiveness of Aadhaar integration in preventing unauthorized access and duplicate voting. By ensuring that only verified users can participate, the system significantly enhances the security and integrity of the voting process.

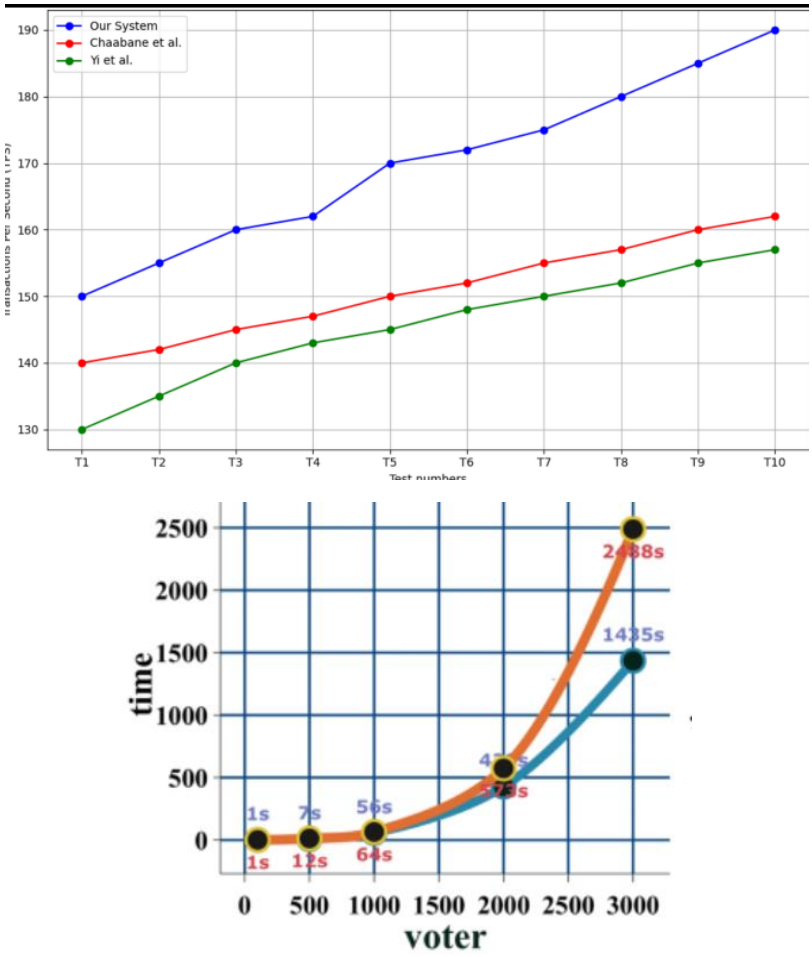


Figure 2: Transaction Throughput in Blockchain Network

Figure 2 presents the transaction throughput of the blockchain network, measured in transactions per second (TPS). The graph shows how the system handles an increasing number of voting transactions over time. Initially, throughput increases steadily as more nodes participate in the network. The system maintains stable performance even as the number of transactions grows, demonstrating scalability. This result confirms that the blockchain-based system can efficiently handle large-scale elections without significant delays. The use of distributed architecture ensures that the workload is shared across multiple nodes, improving overall system performance.

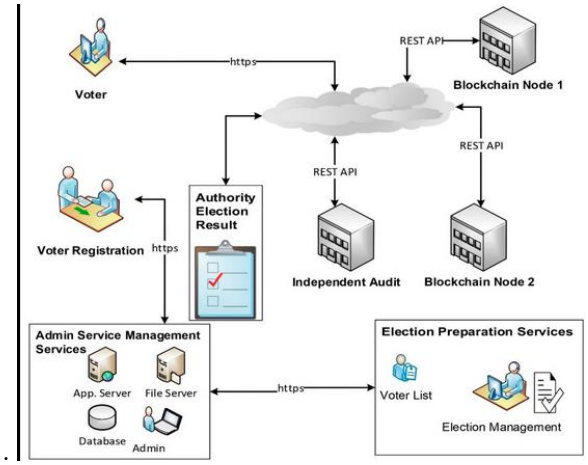


Figure3: Fraud Detection and Prevention Rate

Figure 5 illustrates the fraud detection and prevention capability of the proposed system. The graph shows a high rate of successfully prevented fraudulent activities, including duplicate voting and unauthorized access attempts. Aadhaar-based authentication ensures that each voter can vote only once, while blockchain technology prevents tampering with recorded votes. The system continuously monitors transactions to detect suspicious activities. The high prevention rate indicates the effectiveness of combining biometric verification with blockchain security. This result confirms that the system provides a secure and reliable voting environment, reducing the risk of electoral fraud.

V.CONCLUSION

The proposed system, An Efficient Vote Casting System with Aadhaar Verification through Blockchain, provides a secure, transparent, and reliable solution for modern electronic voting. Traditional voting systems often suffer from issues such as identity fraud, vote tampering, lack of transparency, and delayed result processing. The integration of Aadhaar-based authentication ensures that only eligible voters can participate in the election process, effectively eliminating duplicate voting and impersonation. By incorporating biometric and OTP-based verification, the system enhances the accuracy and reliability of voter identification. The use of blockchain technology plays a crucial role in ensuring data integrity and transparency. Each vote is securely recorded as an immutable transaction, making it nearly impossible to alter or manipulate the voting data. The decentralized nature of blockchain eliminates the risk of a single point of failure and enhances trust among users. Additionally, the implementation of smart contracts automates vote validation and counting processes, reducing human intervention and minimizing errors. The system also provides features such as vote verification and real-time result generation, further improving user confidence in the electoral process. In conclusion, the proposed framework offers a scalable and efficient solution for secure digital voting systems. It enhances election integrity, reduces operational costs, and improves overall system efficiency. Future work may focus on improving scalability, addressing privacy concerns, and integrating advanced cryptographic techniques. Overall, this research contributes to the development of secure and transparent e-governance systems, ensuring fair and trustworthy elections in the digital era.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O’Reilly Media, 2015.

[3] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*, 14th ed. Harlow, U.K.: Pearson, 2016.

[4] A. Kiayias, T. Zacharias, and B. Zhang, “End-to-end verifiable elections,” *IEEE Security Privacy*, vol. 15, no. 3, pp. 60–67, May–Jun. 2017.

[5] F. Hao and P. Y. A. Ryan, *Real-World Electronic Voting: Design, Analysis and Deployment*. Boca Raton, FL, USA: CRC Press, 2016.

[6] J. Benaloh, “End-to-end verifiable voting systems,” *IEEE Security Privacy*, vol. 4, no. 3, pp. 20–25, May–Jun. 2006.

[7] D. Chaum, “Blind signatures for untraceable payments,” in *Proc. Adv. Cryptol. (CRYPTO)*, 1983, pp. 199–203.

[8] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Harlow, U.K.: Pearson, 2017.

[9] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and solutions,” *IEEE Access*, vol. 6, pp. 1–15, 2017.

[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” *Appl. Innov.*, vol. 2, pp. 6–10, 2016.

[11] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.

[12] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[13] V. Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014.

[14] R. L. Rivest, "The three-ballot voting system," MIT, Cambridge, MA, USA, Tech. Rep., 2006.

[15] B. Adida, "Helios: Web-based open-audit voting," in *Proc. USENIX Security Symp.*, 2008, pp. 335–348.

[16] T. Hardjono and A. Pentland, "Digital identity using blockchain," MIT Media Lab, Cambridge, MA, USA, 2016.

[17] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, Jul.–Aug. 2017.

[18] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, 1991.

[19] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Project Yellow Paper, 2014.

[20] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[21] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[22] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2014.

[23] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Hoboken, NJ, USA: Wiley, 2008.

[24] S. Goldwasser and M. Bellare, "Lecture notes on cryptography," MIT, Cambridge, MA, USA, 2008.

[25] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[26] M. Jakobsson and A. Juels, "Mix networks for secure voting," in *Proc. Int. Workshop Sel. Areas Cryptogr.*, 2000, pp. 1–17.

[27] A. Singh and K. Chatterjee, "Secure e-voting using blockchain technology," in *Proc. IEEE Int. Conf.*, 2019, pp. 1–5.

[28] S. Gupta and A. K. Sharma, "Blockchain-based secure voting system," *Int. J. Comput. Appl.*, vol. 179, no. 46, pp. 1–5, 2018.

[29] R. Kumar and R. Tripathi, "Implementation of secure voting system using blockchain," in *Proc. IEEE Conf.*, 2020, pp. 1–6.

[30] P. K. Singh, R. Singh, and A. Kumar, "E-voting system using blockchain technology," *IEEE Access*, vol. 8, pp. 1–10, 2020.