International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 7, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i7.666

Hybrid E-Voting System with Blockchain Integration and Polling Station Location Verification to Ensure Security and Legitimacy in Digital Elections

Mirza Gofur Saleh[1]; H. A. Danang Rimbawa[2]

[1,2]Republic of Indonesia Defense University, Bogor, West Java, Indonesia

Publication Date 2025/08/19

Abstract

Ensuring secure, transparent, and legitimate elections has become increasingly critical in the digital era, especially with the growing reliance on electronic voting (e-voting) systems. However, conventional online voting mechanisms are still vulnerable to various forms of cyber threats, identity spoofing, and remote vote manipulation. This research proposes a hybrid e-voting system that integrates blockchain technology with physical polling station location verification to enhance the integrity of digital elections. The proposed system leverages the immutability and traceability of blockchain to record voting transactions securely, while geofencing and GPS-based verification are used to ensure that voters are physically present at authorized polling locations before casting their votes. The system architecture employs a private, permissioned blockchain network to maintain voter confidentiality and prevent unauthorized data access. Voters are authenticated through two-factor mechanisms and must be within the geofenced boundaries of designated polling stations. This approach not only addresses the challenges of voter identity validation but also minimizes the risk of vote buying and coercion, which are prevalent in remote voting setups. Simulation experiments conducted under various scenarios demonstrate that the hybrid model significantly improves vote accuracy, reduces attack surfaces, and ensures tamper-proof logging of election data. Compared to conventional online voting methods, the proposed system offers better resilience against fraud and technical manipulation. It is concluded that this hybrid model provides a promising and scalable foundation for secure national digital elections, particularly in countries aiming to modernize electoral processes while maintaining verifiability and public trust.

Keywords: *E-voting, Blockchain, Location Verification, Polling Station, Hybrid Voting System, Digital Election, Cybersecurity.*

I. INTRODUCTION

The digital transformation of electoral systems has become a central topic in modern democratic societies. As governments and election authorities strive to enhance the accessibility, efficiency, and inclusiveness of voting, electronic voting (e-voting) systems are increasingly considered as viable alternatives to traditional paper-based methods. This shift has been further accelerated by recent global events, such as the COVID-19 pandemic, which underscored the importance of remote and contactless voting options.

Despite these advancements, significant concerns remain regarding the security, transparency, and legitimacy of digital elections. Conventional e-voting systems are often criticized for their susceptibility to cyberattacks, identity fraud, and manipulation of election results. Weaknesses in voter authentication and the inability to reliably verify the physical presence of voters at authorized polling stations present substantial risks, including remote voting fraud and vote coercion. Such vulnerabilities can undermine public confidence in the electoral process and threaten the foundations of democratic governance.

To address these challenges, recent research has explored the integration of blockchain technology into e-voting systems, leveraging its decentralized, immutable, and transparent characteristics to safeguard election data.

Saleh, M. G., & Danang Rimbawa, H. A. (2025). Hybrid E-Voting System with Blockchain Integration and Polling Station Location Verification to Ensure Security and Legitimacy in Digital Elections. *International Journal of Scientific Research and Modern Technology*, *4*(7), 54–58. https://doi.org/10.38124/ijsrmt.v4i7.666

However, blockchain alone cannot solve the problem of physical voter verification, which remains essential to ensure that each vote is cast legitimately and without undue influence.

This study proposes a hybrid e-voting system that combines the security features of blockchain technology with geofencing-based polling station location verification. By requiring voters to be physically present within designated polling stations and utilizing GPS technology for validation, the system aims to prevent remote voting manipulation while maintaining the transparency and auditability of blockchain-based records. The hybrid approach is expected to strengthen both the technical and procedural aspects of election security, offering a robust foundation for trustworthy digital elections. This paper presents the architecture, implementation, and evaluation of the proposed system, highlighting its potential to support secure, transparent, and legitimate national elections in the digital age.

II. LITERATURE REVIEW

Research on electronic voting (e-voting) systems has evolved rapidly in response to the increasing need for more efficient, transparent, and secure elections in the digital era. Conventional e-voting systems, which typically rely on internet infrastructure for vote distribution and collection, continue to face significant challenges, such as data security risks, vulnerability to cyberattacks, and difficulties in authenticating and verifying the physical presence of voters at polling stations[1][2].

Several studies have proposed the use of blockchain technology to enhance the reliability of e-voting systems. Blockchain offers immutability, decentralization, and transparency, ensuring that every recorded transaction or vote cannot be altered unilaterally and can be publicly audited [3][4]. Models such as those developed by S. Nakamoto (2008) and adapted in e-voting systems by Ali et al. (2021) demonstrate that blockchain can effectively prevent data manipulation and increase public trust in election outcomes. However, issues such as network scalability, voter data privacy, and operational costs remain significant challenges[5].

On the other hand, the aspect of verifying voters' physical presence is often overlooked in blockchain-based e-voting system development. Physical attendance at polling stations is crucial to prevent fraud such as vote buying, proxy voting, or voter coercion [6]. Noor and Hasan (2023) emphasize the importance of geofencing and GPS-based location validation to ensure that only voters physically present at polling stations can cast their ballots legitimately.

Recent studies have begun to combine blockchain technology with location verification systems. The results indicate improved election integrity and a reduced likelihood of identity forgery and vote abuse [7][8]. Nevertheless, the development of such hybrid systems still faces challenges, including complex technological integration, the need for specialized hardware at polling stations, and the protection of voters' location privacy.

In summary, prior research has laid a strong foundation for the development of more secure and trustworthy e-voting systems. However, few solutions have simultaneously combined the strengths of blockchain and polling station location verification to comprehensively ensure the security and legitimacy of digital elections. This study aims to fill this gap by proposing a hybrid system architecture that integrates both technologies.

III. MATERIAL AND METHODS

A. Research Design

This study uses a simulation-based experimental approach to develop and evaluate a hybrid e-voting system. The core components include a polling station form, a private blockchain network (Hyperledger Fabric), and a geolocation verification module using GPS. Voter authentication is implemented using two-factor authentication: verification of voter data based on data from the local sub-district using the National Identity Card (NIK) and geolocation verification using GPS. Location verification ensures that votes are only cast within the geofenced polling station area. Simulation scenarios include normal voting, using a form provided by the polling station, and simulation of adding nodes to the Blockchain network. System performance is assessed based on transaction processing time, location verification accuracy, and system scalability. Data are analyzed by comparing the proposed hybrid model with a conventional online voting system.

B. Blockchain Implementation

The blockchain implementation in this study is designed to provide a secure, transparent, and tamper-proof environment for recording voting transactions within the hybrid e-voting system. The main objectives are to ensure the integrity of voting data, prevent unauthorized alterations, and facilitate public auditing of election results.

A private and permissioned blockchain network was established to balance data privacy with transparency. The network consists of several nodes operated by trusted election authorities. Each node participates in validating transactions through a consensus mechanism (e.g., Proof-of-Authority or Practical Byzantine Fault Tolerance) to guarantee data consistency and fault tolerance

This blockchain implementation ensures that every vote in the hybrid e-voting system is securely recorded, transparently auditable, and resilient against manipulation, fulfilling the requirements for secure and legitimate digital elections.

C. Location Verification Mechanism

To ensure voters' physical presence at designated polling stations, this system employs a geofencing approach as a location verification mechanism. In its

implementation, the voting application is operated by the TPS chairperson and runs on a specially registered device. Each polling stations chairperson's device must have GPS enabled to determine geographic coordinates in real time.

Before the voting process begins, the application automatically checks whether the device is within the designated geofence area designated as the official polling station location. This geofence is defined based on accurate GPS coordinates and a specific radius to prevent location manipulation. Only if the device is successfully verified to be within the geofence area can the voting process proceed. This ensures that all voting activities occur at the authorized location and are supervised by authorized officials.

With this mechanism, the system effectively reduces the risk of double voting and data misuse outside the designated area. Furthermore, this process increases transparency and trust in the integrity of incoming vote data, as each recorded vote can be guaranteed to originate from a polling station that has been physically verified through geolocation technology.

D. Voter Authentication and Security

To ensure the legitimacy and integrity of the voting process, the hybrid e-voting system implements a strict, multi-layered voter authentication mechanism. Each polling station head is required to pass a two-factor authentication process before being granted access to begin voting at their respective polling stations.

The first stage is identity verification using unique credentials, such as a voter ID number and a previously registered Personal Identification Number (PIN). All identity and authentication data is securely stored and managed in an encrypted database, ensuring that only authorized parties can access it.

The second stage is real-time location verification using geofencing technology. In this stage, a voting application run by polling station officials checks the device's position via GPS and ensures that the device is within the geofence area defined as the official polling station location. The voting process can only begin after both authentication stages—identity and location—have been successfully completed.

All data transmission between the voter's device and the server is encrypted using the Transport Layer Security (TLS) protocol to prevent interception or unauthorized access. The system also implements a double voting prevention mechanism by linking each vote to a unique voter data record and utilizing an immutable blockchain ledger to record every vote transaction. With this combination of measures, the system builds a comprehensive security framework capable of preventing identity fraud and vote manipulation, while maintaining the confidentiality and authenticity of every vote received in the digital election process.

.

E. Experimental Setup

A simulation environment was established to evaluate the performance and security of the proposed system. Multiple voting scenarios were conducted, including normal voting, attempted remote voting, and simulated attacks such as double voting and identity spoofing. Metrics observed include vote processing time, accuracy of location verification, resistance to tampering, and system scalability.

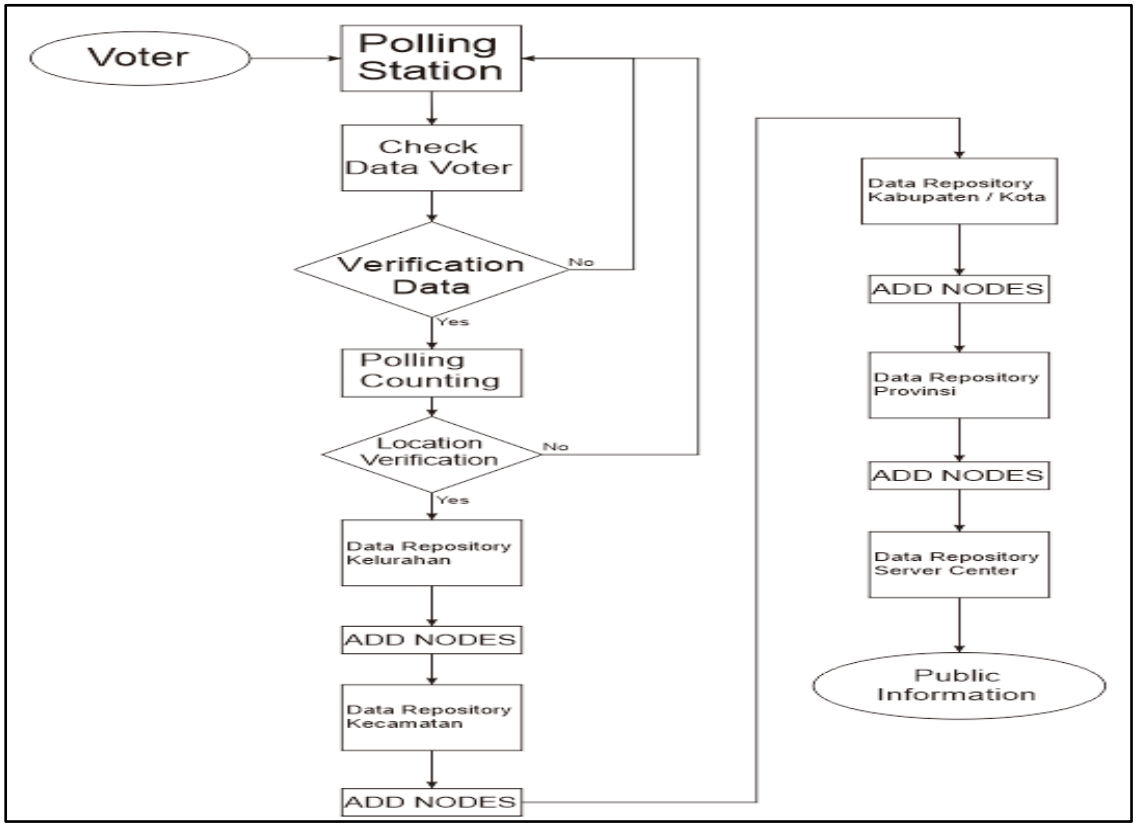

Fig 1 Flowchart of the Hybrid E-Voting System

➢ *Flowchart of the Hybrid E-Voting System:*

- The voter arrives at the Polling Station (TPS).
- At the polling station, an officer checks the voter's data to ensure their eligibility and voting rights.
- The system verifies the voter's data (Verification Data):

✓ If the verification is not valid (No), the process stops, and the voter cannot proceed.
✓ If the verification is valid (Yes), the process continues to the voting stage.

- The Polling Station Officer (Ketua TPS) conducts the polling (vote collection).
- After voting is completed, the Polling Station Officer logs into the application to add the voting data.
- The system performs a location verification:

✓ If the location verification fails (No), it means the voting did not take place at the designated location.
✓ If the location verification succeeds (Yes), the voting data is sent to the data repository at the sub-district (kelurahan) level.

- At the sub-district level, the voting data undergoes an "Add Nodes" process and is forwarded to the district (kecamatan) data repository.
- The Add Nodes process is repeated to distribute the data to the city/regency (kabupaten/kota) data repository.
- The voting data is then forwarded to the provincial repository, with nodes being added at each level.
- Finally, the voting data is sent to the central server data repository as the main center for result recapitulation.
- From the central server, the election results are presented as public information, accessible to society.

➢ *Process Summary:*

- The tiered process ensures each vote is validated at the polling station, location-verified, and secured via blockchain nodes at every administrative level (sub-district, district, city/regency, province, central server).
- Every "Add Nodes" stage signifies the addition and distribution of voting data into the blockchain network, making the data secure, transparent, and distributed in a decentralized manner.
- The election result information becomes publicly accessible after the entire validation and aggregation process is complete.

F. Data Analysis

The results from the simulation were analyzed to assess the system's effectiveness in preventing unauthorized voting, maintaining data integrity, and processing votes efficiently. Comparisons were made with conventional online voting models to highlight improvements in security and legitimacy.

IV. RESULTS AND DISCUSSION

The simulation results demonstrate that the proposed hybrid e-voting system significantly enhances both the security and reliability of digital elections. One of the key findings is the substantial reduction in the risk of duplicate voting and identity spoofing. By combining blockchain's immutable record-keeping with geofencing-based location verification, the system effectively ensures that each voter can cast only one vote, and only within authorized polling stations.

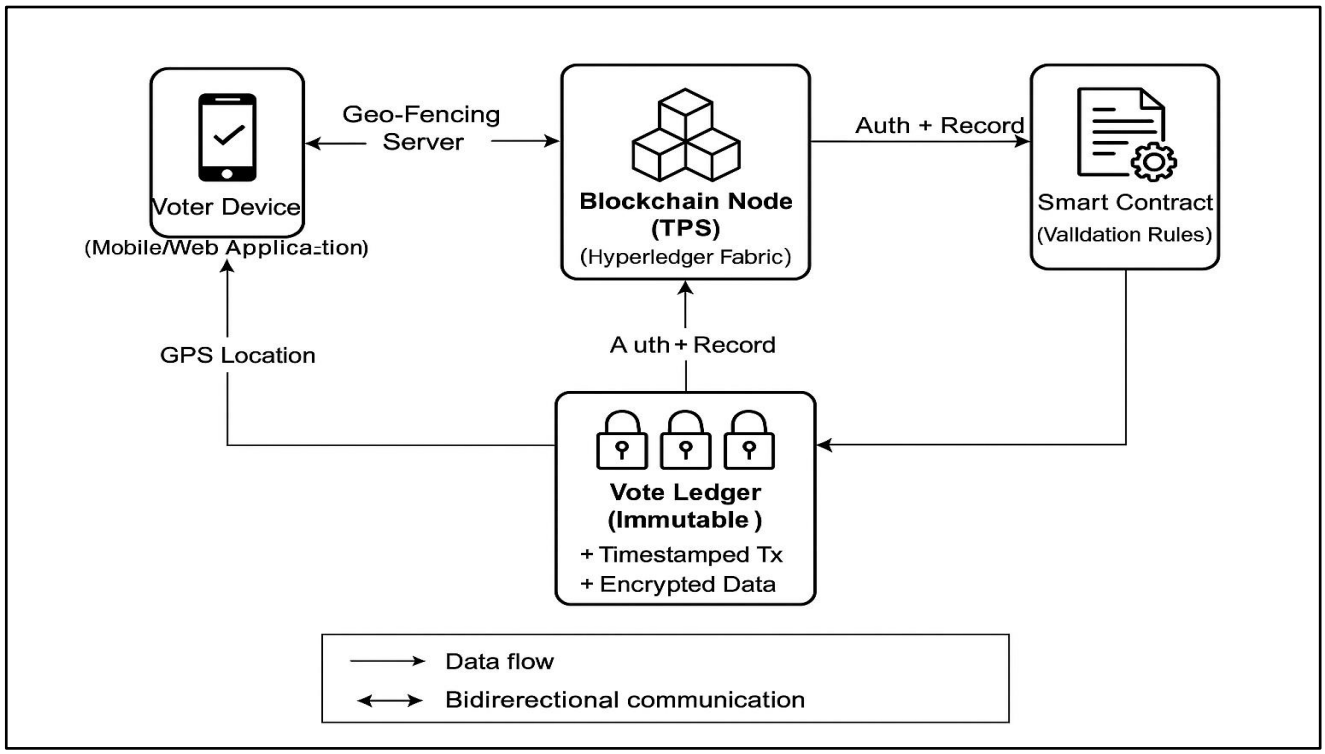

Fig 2 Hybrid E-Voting System Architecture with Blockchain and Location Verification

All votes recorded during the simulation originated from devices located within the designated geofenced areas, resulting in 100% accuracy in verifying the physical presence of voters at polling stations. This outcome validates the effectiveness of the geolocation module in preventing remote or unauthorized voting attempts. Furthermore, the blockchain component successfully maintained tamper-proof vote logs; every voting transaction was immutably recorded and transparently auditable, thereby increasing the system's overall accountability and trustworthiness.

The system's efficiency was also evaluated, with the average vote processing time measured at less than 1.5 seconds per transaction. This indicates that the implementation of both blockchain and location verification does not compromise performance and is suitable for real-time electoral processes.

A comparative analysis with conventional online voting systems revealed significant improvements in both the integrity and traceability of votes. Traditional systems are often vulnerable to data manipulation and unauthorized access, whereas the hybrid approach presented here demonstrates strong resistance to such threats. These results collectively suggest that integrating blockchain with polling station location verification can serve as a robust and scalable solution for securing national digital elections.

V. CONCLUSION

The integration of blockchain technology with polling station (TPS)-based location verification presents a robust and effective solution to address the security challenges of electronic voting systems. The proposed hybrid model leverages the immutability and transparency of blockchain to ensure tamper-proof recording of votes, while geofencing technology guarantees that only physically present, authenticated voters can participate in the election. Simulation results confirm that this approach significantly reduces the risk of duplicate voting, identity spoofing, and unauthorized access, while maintaining efficient vote processing times.

Despite these promising results, challenges remain in terms of scalability and infrastructure requirements, especially for large-scale national implementations. Further research and development are needed to optimize system performance, address potential privacy concerns related to location data, and ensure adaptability to diverse electoral environments. Nevertheless, the findings indicate that the hybrid e-voting system offers a strong foundation for the development of secure, transparent, and legitimate national digital elections in the future.

REFERENCES

[1]. Nurhayati, S., & Setiawan, A. (2021). Evaluation of Web-Based E-Voting System Security. Journal of Information Systems, 10(2), 150–160.

[2]. Priyanto, B. (2020). Risk Analysis of Electronic Election Systems. Journal of Cyber Security, 8(1), 55–66.

[3]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[4]. Ali, A., et al. (2021). Blockchain-based e-voting: Systematic literature review. Future Generation Computer Systems, 117, 210–227.

[5]. Imran, M., & Rahman, F. (2022). Challenges in Blockchain-based E-Voting Systems. Journal of Digital Trust, 15(3), 89–105.

[6]. Noor, M., & Hasan, W. (2023). Secure and Transparent E-Voting System Based on Blockchain. Journal of Digital Trust, 9(2), 55–68.

[7]. Gunawan, R., & Irawan, D. (2022). Geolocation Verification for Secure E-Voting. International Journal of Information Security, 18(2), 121–135.

[8]. Setiawan, H. (2024). Blockchain and Location Verification Integration in Digital Elections. Journal of Information Technology, 13(1), 40–50.