



A Blockchain-Based Security Model for Enhancing Data Integrity and Privacy in Vehicular Ad Hoc Networks

Mercy Ayosi Fred^{1*}, Siman Emmanuel², Baaku Raphael³

Kwararafa University, Wukari.

*Corresponding Author

Mercy Ayosi Fred

Article History

Received: 11.06.2026
Revised: 08.07.2026
Accepted: 22.08.2026
Published: 16.09.2026

Abstract: Vehicular Ad Hoc Networks (VANETs) provide communication between vehicles and roadside infrastructure for safety, traffic management, and intelligent transportation applications. However, the highly dynamic nature of VANETs exposes vehicular communication to security threats including unauthorized access, spoofing, Sybil attacks, data tampering, and privacy violations. This study presents a blockchain-based security model for enhancing data integrity, privacy, authentication, and communication reliability in VANETs. The proposed framework integrates a blockchain layer with a Modified Stable Weighted Clustering (m-SWC) algorithm, cryptographic authentication, pseudonymous identities, and a consensus mechanism. The model was evaluated through simulation under different vehicle densities and attack conditions. Performance was assessed using packet delivery ratio, end-to-end delay, authentication success rate, attack rejection, communication overhead, and scalability. The results show that the proposed blockchain-enabled VANET achieves higher and more stable packet delivery performance than conventional approaches. Authentication performance also improved, with the Blockchain VANET achieving a 97% authentication success rate and 95% attack rejection compared with 86% and 78%, respectively, for the PKI system. The results further show that blockchain introduces moderate additional latency because of consensus and verification processes, but the delay remains within acceptable limits for real-time vehicular applications. The system also demonstrates controlled communication overhead and robust scalability as the number of vehicles increases from 50 to 200. The study therefore demonstrates that blockchain integration provides an effective balance between security, reliability, and scalability in VANET environments.

Keywords: Blockchain, VANET, Data Integrity, Privacy, Authentication, Modified Stable Weighted Clustering, PBFT, Vehicular Networks.

This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/) (CC BY-NC 4.0)

Cite this article:

Fred, M. A., Emmanuel, S., Raphael, B., (2026). A Blockchain-Based Security Model for Enhancing Data Integrity and Privacy in Vehicular Ad Hoc Networks. *ISAR Journal of Science and Technology*, 4(9), 40-44.

1.0 Introduction

Vehicular Ad Hoc Networks are an important component of intelligent transportation systems because they enable vehicles to exchange information with other vehicles and roadside infrastructure. Such communication supports applications including collision avoidance, emergency notification, traffic coordination, and other safety-critical services.

Despite these benefits, VANET communication is vulnerable to security and privacy threats. The dynamic topology, high mobility of vehicles, and dependence on distributed communication create opportunities for malicious nodes to inject false information, modify messages, impersonate legitimate vehicles, or obtain sensitive information.

Traditional security approaches such as Public Key Infrastructure (PKI) and centralized authentication can provide protection but may introduce dependence on centralized trust authorities and potential bottlenecks. The literature reviewed in the study identifies the need for security mechanisms capable of balancing security, resource consumption, scalability, and real-time performance.

Blockchain provides a decentralized and tamper-resistant mechanism for recording and validating transactions. In the proposed framework, blockchain is combined with Modified Stable Weighted Clustering to improve secure communication and network stability.

1.1 Research Problem

Existing VANET security mechanisms face challenges involving centralized trust, data tampering, unauthorized access, privacy exposure, and scalability. Security mechanisms that focus only on authentication or privacy may not adequately address the broader requirements of secure vehicular communication.

Therefore, this study proposes a blockchain-based security model that combines decentralized authentication, immutable data storage, privacy-preserving mechanisms, consensus validation, and m-SWC-based network organization.

1.2 Aim of the Study

The aim of this study is to develop a blockchain-based security model for enhancing data integrity and privacy in Vehicular Ad Hoc Networks.

1.3 Research Objectives

Develop a blockchain-based security framework for secure V2V and V2I communication.

Integrate Modified Stable Weighted Clustering to improve network stability and data forwarding.

Implement decentralized authentication using blockchain technology.

Evaluate the proposed framework in terms of communication performance, security, latency, and scalability.

2.0 Related Work and Research Gap

Previous studies have investigated blockchain, authentication, privacy-preserving mechanisms, and trust management for VANETs. Blockchain has attracted attention because its decentralized ledger can provide immutable records and support verification without depending entirely on a centralized authority.

However, the literature indicates continuing challenges involving computational requirements, scalability, and latency. Existing studies frequently concentrate on individual security concerns such as authentication or privacy rather than providing an integrated framework addressing security and network performance simultaneously.

The research gap addressed by this study is therefore the integration of blockchain-based security with network optimization through Modified Stable Weighted Clustering, with the objective of achieving secure, reliable, and scalable vehicular communication.

3.0 Proposed Methodology

The proposed architecture consists of vehicles, Roadside Units (RSUs), and a blockchain layer. Vehicles communicate through Vehicle-to-Vehicle and Vehicle-to-Infrastructure links. RSUs perform validation and participate in the blockchain network, while blockchain nodes maintain immutable transaction records.

3.1 Blockchain Security Layer

The blockchain layer provides decentralized authentication, message verification, and immutable transaction storage. This helps prevent unauthorized modification of transmitted information and provides traceability for validated transactions.

3.2 Modified Stable Weighted Clustering

The m-SWC algorithm is used to form stable vehicle clusters and support efficient packet forwarding and recovery. Stable clustering helps reduce communication disruption resulting from vehicle mobility and network instability.

3.3 Privacy Preservation

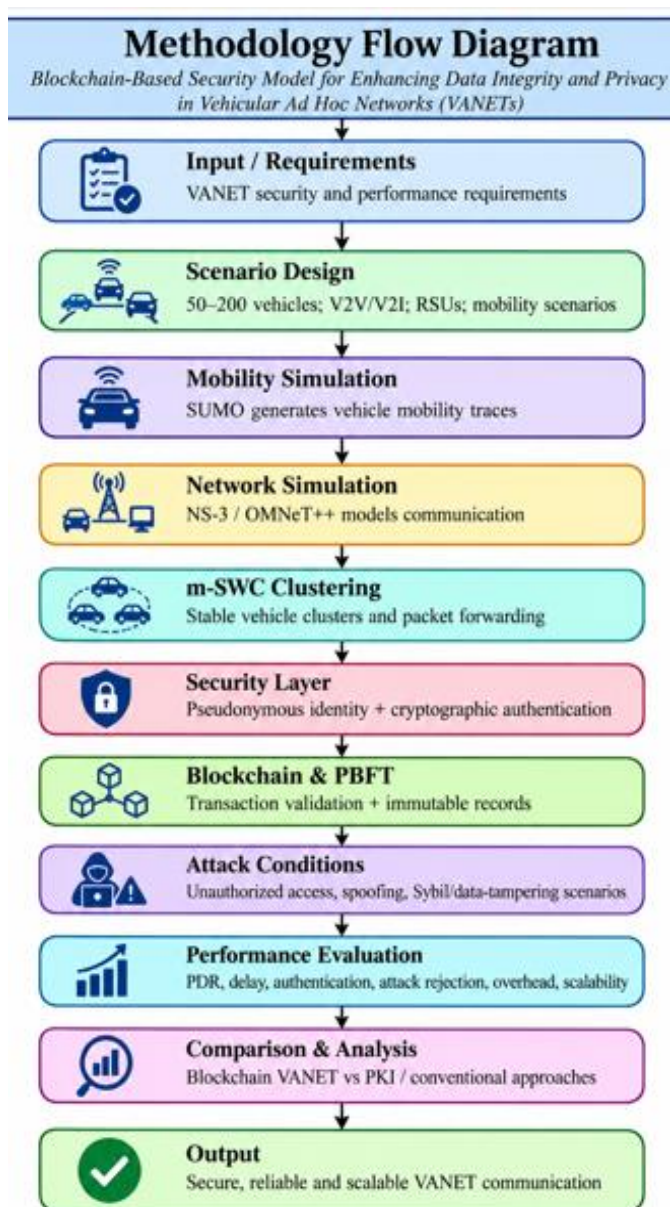
The framework uses cryptographic mechanisms and pseudonymous identities to protect vehicle-related information such as location and speed from unauthorized parties.

3.4 Consensus

PBFT is used in the simulation to provide agreement among blockchain participants while supporting low-latency transaction validation. The simulation considered 50–200 vehicles, block times of 2–5 seconds, packet sizes of 256–1024 bytes, and medium-to-high RSU density.

3.5 Simulation Environment

The study used NS-3 and SUMO for network and mobility simulation, with OMNeT++ supporting communication-layer simulation. The blockchain layer was represented using Hyperledger Fabric/private Ethereum, with Python and C++ used for implementation. The experimental hardware included an Intel Core i7/Ryzen 7 processor, 16 GB RAM, and 512 GB SSD.



4.0 Results and Discussion

4.1 Packet Delivery Ratio

The proposed blockchain-enabled VANET consistently achieved higher and more stable packet delivery performance than conventional approaches across different vehicle densities. The improvement is associated with blockchain authentication and verification, which filter malicious and unauthorized nodes before packet dissemination. The system remained relatively stable even as vehicle density increased.

4.2 End-to-End Delay

End-to-end delay increased as vehicle density increased because of greater channel contention and processing demands. The blockchain model introduced moderate additional latency compared with conventional PKI approaches because of transaction validation and consensus processing. However, the delay remained within acceptable limits for safety-critical VANET applications.

4.3 Authentication Performance

The authentication results demonstrate a clear improvement:

Model	Authentication Success	Attack Rejection
PKI System	86%	78%
Blockchain VANET	97%	95%

The Blockchain VANET improved authentication success from 86% to 97% and attack rejection from 78% to 95%. This improvement is attributed to decentralized identity verification against immutable blockchain records, enabling unauthorized or spoofed identities to be detected before network admission.

4.4 Communication Overhead

Communication overhead increased gradually with vehicle density because more vehicles generated additional authentication requests, consensus operations, and blockchain transactions. However, the distributed architecture spreads the communication load across RSUs and blockchain nodes, reducing the possibility of a single processing bottleneck.

4.5 Scalability

The scalability analysis considered networks ranging from 50 to 200 vehicles. The system remained stable at low and medium densities. Beyond approximately 150 vehicles, verification time and end-to-end delay increased slightly because the PBFT mechanism had to process more transactions. Nevertheless, packet delivery and throughput remained within acceptable operational limits, and the degradation was gradual rather than abrupt.

4.6 Comparative Analysis

Model	Security	Latency	PDR	Scalability
PKI	Medium	Low	Medium	Low
Centralized	Medium	Medium	Medium	Medium
Blockchain VANET	High	Moderate	High	High

The proposed Blockchain VANET provides stronger security, higher packet delivery performance, and better scalability, while introducing moderate latency because of blockchain verification and consensus.

5.0 Discussion

The findings demonstrate that blockchain integration improves VANET security through decentralized authentication, tamper-resistant data storage, and message verification. Higher PDR and authentication performance indicate that malicious and unauthorized nodes can be filtered before participating in communication.

The main trade-off is latency. Blockchain consensus introduces additional processing compared with conventional authentication mechanisms. However, the study reports that the additional latency remains within acceptable limits for real-time vehicular applications.

RSU density also affects system performance. Higher RSU density can improve verification speed and reduce communication delay, although it increases infrastructure requirements and deployment complexity.

6.0 Conclusion

This study developed and evaluated a blockchain-based security model for enhancing data integrity, privacy, authentication, and communication reliability in VANETs. The framework combines blockchain, decentralized authentication, privacy-preserving identities, PBFT consensus, and Modified Stable Weighted Clustering.

The simulation results demonstrate that the proposed approach achieves higher packet delivery performance and substantially improved authentication compared with the PKI model. The Blockchain VANET achieved 97% authentication success and 95% attack rejection, compared with 86% and 78% for PKI.

Although blockchain introduces moderate latency and communication overhead, the system maintains acceptable performance as network size increases. The gradual degradation beyond approximately 150 vehicles indicates that the proposed architecture remains scalable rather than experiencing an abrupt centralized bottleneck.

Overall, the findings support the use of blockchain combined with clustering-based optimization as a promising

approach for secure and scalable intelligent transportation systems.

6.1 Contribution to Knowledge

The research contributes by integrating blockchain technology with Modified Stable Weighted Clustering for VANET security. The framework addresses authentication, data integrity, privacy, and network efficiency within a unified architecture rather than treating these concerns independently.

6.2 Future Work

Future research should validate the framework using large-scale real-world vehicular testbeds and investigate lightweight consensus mechanisms to reduce computational and communication overhead. Integration with edge computing, 5G/6G networks, and machine-learning-based intrusion detection may further improve scalability and responsiveness.

References

1. Ahmed, W., & Di, W. (2022). Privacy-preserving blockchain-based authentication and trust management in VANETs. **IET Networks**. <https://doi.org/10.1049/ntw2.12036>
2. Alladi, T., Chamola, V., Sahu, N., Venkatesh, V., Goyal, A., & Guizani, M. (2022). A comprehensive survey on the applications of blockchain for securing vehicular networks. **IEEE Communications Surveys & Tutorials**, 24*(2), 1212–1239. <https://doi.org/10.1109/COMST.2022.3160925>
3. Dwivedi, S. K., Amin, R., Das, A. K., Leung, M. T., Choo, K.-K. R., & Vollala, S. (2022). Blockchain-based vehicular ad-hoc networks: A comprehensive survey. **Ad Hoc Networks**, 137*, 102980. <https://doi.org/10.1016/j.adhoc.2022.102980>
4. Ilyas, I., Din, I. U., Alourani, A., & Ashraf, M. U. (2024). Lightweight consortium blockchain-enabled secured Vehicular ad Hoc Network using certificateless conditional privacy-preserving authentication mechanism. **PLOS ONE**, 19*(10), e0310267. <https://doi.org/10.1371/journal.pone.0310267>
5. Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., & Khan, M. K. (2024). A survey on the blockchain techniques for the Internet of Vehicles security. **Transactions on Emerging Telecommunications Technologies**, 35*(4), e4317. <https://doi.org/10.1002/ett.4317>
6. Lu, H., & Li, J. (2016). Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey. **Wireless Communications and Mobile Computing**, 16*(6), 643–655. <https://doi.org/10.1002/wcm.2558>

7. Lu, Z., Liu, W., Wang, Q., Qu, G., & Liu, Z. (2018). A privacy-preserving trust model based on blockchain for VANETs. **IEEE Access*, 6*, 45655–45664. <https://doi.org/10.1109/ACCESS.2018.2864189>
8. Manivannan, D., Moni, S. S., & Zeadally, S. (2020). Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETWORKS (VANETs). **Vehicular Communications*, 25*, 100247. <https://doi.org/10.1016/j.vehcom.2020.100247>
9. Mundhe, P., Verma, S., & Venkatesan, S. (2021). A comprehensive survey on authentication and privacy-preserving schemes in VANETs. **Computer Science Review*, 41*, 100411. <https://doi.org/10.1016/j.cosrev.2021.100411>
10. Ogundoyin, S. O., & Kamil, I. (2021). An efficient authentication scheme with strong privacy preservation for fog-assisted vehicular ad hoc networks based on blockchain and neuro-fuzzy. **Vehicular Communications*, 31*, 100384. <https://doi.org/10.1016/j.vehcom.2021.100384>
11. Saad, M., Khan, M. K., & Ahmad, M. B. (2022). Blockchain-enabled vehicular ad hoc networks: A systematic literature review. **Sustainability*, 14*(7), 3919. <https://doi.org/10.3390/su14073919>
12. Shawky, M. A., Jabbar, A., Usman, M., Imran, M., Abbasi, Q. H., Ansari, S., & Taha, A. (2023). Efficient blockchain-based group key distribution for secure authentication in VANETs. **IEEE Networking Letters*, 5*(1), 64–68. <https://doi.org/10.1109/LNET.2023.3234491>
13. Son, S., Lee, J., Park, Y., Park, Y., & Das, A. K. (2022). Design of blockchain-based lightweight V2I handover authentication protocol for VANET. **IEEE Transactions on Network Science and Engineering*, 9*(3), 1346–1358. <https://doi.org/10.1109/TNSE.2022.3142287>
14. Soujanya, B. K., & Azam, F. (2024). Ensuring security and privacy in VANET: A comprehensive survey of authentication approaches. **Journal of Computer Networks and Communications*, 2024*, 1818079. <https://doi.org/10.1155/2024/1818079>
15. Yang, Y., Wei, L., Wu, J., Long, C., & Li, B. (2022). A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network. **IEEE Internet of Things Journal*, 9*(11), 8078–8090. <https://doi.org/10.1109/JIOT.2021.3107443>