Blockchain-Enabled Intrusion Detection System for Distributed Vehicular Networks

Hope Leticia Nakayiza, Love Allen Chijioke Ahakonye [†], Dong-Seong Kim, Jae Min Lee,
IT Convergence Engineering, [†] ICT Convergence Research Center,
Kumoh National Institute of Technology Gumi, South Korea
hopeleticia, loveahakonye, dskim, ljmpaul@kumoh.ac.kr

***Abstract*—Security and privacy are critical in vehicular networks due to their sensitivity and high connectivity. This paper proposes a novel framework combining blockchain and federated learning to enhance security and intrusion detection. Through smart contracts, blockchain is implemented to manage vehicle participation, ensuring data integrity and immutability while federated learning facilitates collaborative model training without exposing private data. This integrated approach provides a robust security solution, safeguarding vehicular networks against potential threats.**

***Index Terms*—Blockchain, Federated Learning, Intrusion detection, Vehicular Networks**

I. Introduction

Vehicular Ad-hoc Networks (VANETs), which facilitate vehicle-to-vehicle and vehicle-to-infrastructure communication [1], are integral to intelligent transportation systems (ITS). These interactions utilize the IEEE 802.11p standard, facilitating effective communication between vehicles and roadside units [1]. This connectivity is supported by dedicated short-range communications (DSRC) and cellular vehicle-to-everything (C-V2X) modules [2]. It ensures real-time exchange of information crucial for managing traffic and preventing dangerous incidents.

Intrusion detection systems (IDS) are pivotal in attack detection and safeguarding VANETs [2] by monitoring vehicle operations, detecting various attack types in real-time [3], and provide essential information for mitigation. Blockchain technology, characterized by consensus mechanisms that ensure credibility and data immutability, thus providing tamper-proof records [4], [5], has emerged as a promising solution for enhancing trust and security in various environments.

Various studies have presented a decentralized collaborative cyber-attack detection system based on blockchain to identify malicious networks for network security. A blockchain-based privacy protection system using the proof-of-work consensus was proposed in [6] to ensure secure user registration and two-way authentication in the Internet of Vehicles, addressing the central dependency issues in traditional systems. Additionally, to improve security and automation in Industry 5.0, [7] introduced a blockchain-assisted IDS capable of detecting various cyberattacks on autonomous vehicles, thereby creating a trusted 5G vehicle-to-everything network.

This study builds upon these advancements by integrating blockchain with federated learning to ensure the traceability of vehicular communication, security, integrity, and privacy preservation of sensitive vehicular information. By leveraging the decentralized blockchain, the study overcomes the limitations of conventional approaches.

II. System Methodology

The workflow and system model of the proposed scheme is illustrated in Figure 1.

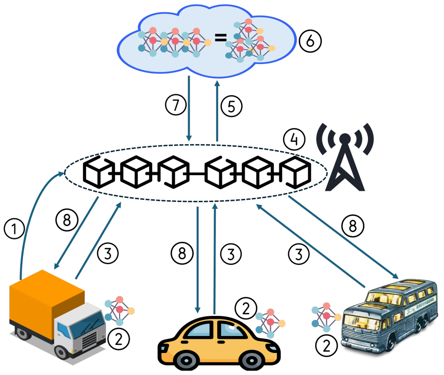

Fig. 1: ①Vehicle Registration on the Blockchain; ②Local Model Training; ③Model updates/IDS results upload; ④Log IDS results, isolate malicious nodes; ⑤Local model updates upload to the cloud server; ⑥Aggregate to form global model; ⑦Global model download; ⑧Global model distribution

A Long short-term memory (LSTM) architecture composed of four fully connected layers was utilized in this study to evaluate the CAN-intrusion dataset [8]. The model's accuracy and computation time were evaluated over 20 rounds, with the number of clients varying between 20 and 60.

A blockchain network was deployed at the roadside unit (RSU) to ensure the secure logging of vehicle information, intrusion detection outcomes, and automatic isolation of malicious nodes. This setup considers vehicles as nodes within the blockchain network, while the RSU acts as the master node, managing vehicle registration and executing smart contracts. A smart contract automates the temporary isolation of identified malicious nodes and maintains an immutable record of all security-related events. The smart contract was deployed using Remix IDE, with Ganache acting as a local Ethereum blockchain environment to effectively simulate Ethereum transactions.

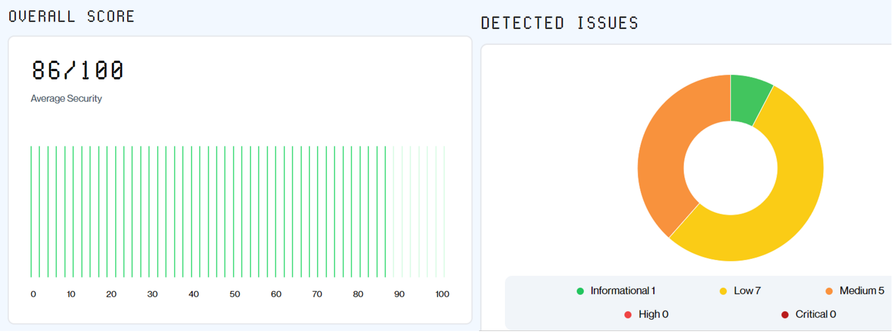

Fig. 2: Smart contract vulnerability check report.

III. Performance Evaluation

Figure 2 is a vulnerability check of the Smart contract utilizing the solidcheck.io, with 86% and no critical threat found. The gas and transaction costs for different functions were also evaluated as presented in Table I. Furthermore, the experimentation results in Figure 3 demonstrate that the model consistently achieved an accuracy of over 99%, with an increasing number of clients, highlighting its scalability and resilience in large-scale vehicular networks.

TABLE I: Gas and Transaction Cost For Vehicle Management Functions on the Blockchain

Function	**Gas**	**Transaction Cost**
registerVehicle	235333	235333
logAlert	142642	142642
isolateVehicle	170624	170624
liftIsolation	37228	32428

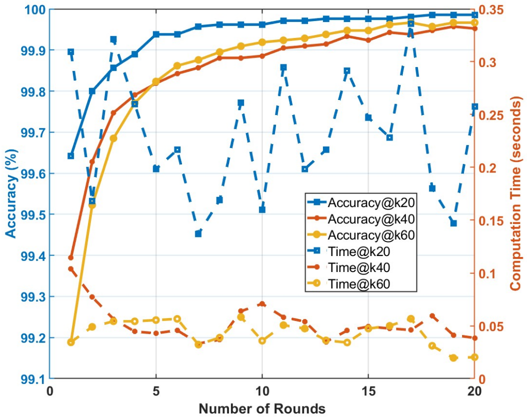

Fig. 3: Graph showing the model's accuracy and time performance across varying client counts over 20 rounds.

IV. Conclusion

This study presents a blockchain-integrated federated learning framework to enhance security, integrity, and traceability in VANETs. Leveraging the decentralized blockchain, the framework effectively mitigates the risk of single points of failure, resulting in a robust and scalable solution for intrusion detection. Integrating smart contracts automates the isolation of malicious nodes, significantly reducing response times to security threats and thus enhancing the overall safety and reliability of VANETs. A future direction is optimizing vehicle communication protocols to reduce latency and enable faster malicious node isolation.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-RS-2020-II201612, 33%) and by the IITP(Institute of Information Communications Technology Planning Evaluation)-ICAN(ICT Challenge and Advanced Network of HRD) grant funded by the Korea government(Ministry of Science and ICT)(IITP-2024-2022-00156394*, 33%) and by the MSIT, Korea, under the ITRC support program(IITP-2024-RS-2024-00438430, 34%) supervised by the IITP

References

[1] H. Tan, S. Xuan, and I. Chung, "HCDA: Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs," *Symmetry*, vol. 12, no. 6, 2020.

[2] J. Nagarajan, P. Mansourian, M. A. Shahid, A. Jaekel, I. Saini, N. Zhang, and M. Kneppers, "Machine Learning Based Intrusion Detection Systems for Connected Autonomous Vehicles: A Survey," *Peer-to-Peer Networking and Applications*, vol. 16, no. 5, pp. 2153–2185, 2023.

[3] G. O. Anyanwu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Novel Hyper-Tuned Ensemble Random Forest Algorithm for the Detection of False Basic Safety Messages in Internet of Vehicles," *ICT Express*, vol. 9, no. 1, pp. 122–129, 2023.

[4] F. Ayaz, Z. Sheng, D. Tian, M. Nekovee, and N. Saeed, "Blockchain-Empowered AI for 6G-Enabled Internet of Vehicles," *Electronics*, vol. 11, no. 20, p. 3339, 2022.

[5] L. Ahakonye, C. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, p. 3111, 05 2024.

[6] T. Su, S. Shao, S. Guo, and M. Lei, "Blockchain-Based Internet of Vehicles Privacy Protection System," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–10, 09 2020.

[7] S. Anbalagan, G. Raja, S. Gurumoorthy, D. Suresh R, and K. Ayyakannu, "Blockchain Assisted Hybrid Intrusion Detection System in Autonomous Vehicles for Industry 5.0," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 4, pp. 881–889, 2023.

[8] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle Network Intrusion Detection using Deep Convolutional Neural Network," *Vehicular Communications*, vol. 21, p. 100198, 2020.