PureChain for Secure Vehicular Edge Computing

Miraculous Udurume[1], Love Allen Chijioke Ahakonye[2], Jae Min Lee[1], Dong-Seong Kim[1]*
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National Institute of Technology*, Gumi, South Korea
*NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
udurumemiraculous@gmail.com, (loveahakonye, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—This paper presents a blockchain-enabled vehicular edge computing system for secure data sharing and intrusion detection. It features a modular design for diverse terrains, blockchain for accountability, and federated learning for data privacy. The system improves scalability, privacy, and security with a simulation-backed Vehicle-to-Vehicle (V2V) communication framework that integrates federated learning, blockchain, and lightweight detection mechanisms. Evaluations with 10, 20, and 30 clients show consistent accuracy above 94% and practical latency-throughput tradeoffs.**

***Index Terms*—Data Sharing, Edge computing, Intrusion Detection, V2V, PoA^2, PureChain,**

I. Introduction

Vehicle-to-Vehicle (V2V) communication is essential for modern intelligent transportation systems (ITS), enabling real-time messaging for collision avoidance, platooning, and cooperative lane changes [1]. Traditional V2V systems rely on centralized infrastructure for authentication and anomaly monitoring [2], [3], but this introduces risks such as single points of failure, scalability limitations, and delayed threat detection. A shift towards decentralized, real-time, and privacy-preserving approaches is necessary [4]. Blockchain offers secure, tamper-proof communication, while federated learning enables decentralized, privacy-preserving model training across autonomous nodes [5], [6]. V2V systems also require low-latency consensus mechanisms for efficient operation.

Integrating blockchain with Intrusion Detection Systems (IDS) improves anomaly detection, enhancing data authenticity and security [2], [5]. The SecNet-FLIDS model [7] combines blockchain and federated learning for secure, privacy-conscious cyberattack detection in the Internet of Vehicles (IoV). This research presents a federated learning-driven IDS backed by PureChain, a custom blockchain based on proof of authority and association consensus mechanism (PoA^2) [8]. It enables secure model aggregation without data exchange and provides immutable logging for trust and traceability. This architecture ensures timely threat detection while preserving privacy in vehicular environments [7], [9].

II. System Architecture

The proposed framework adopts a four-layered architecture for secure and decentralized Vehicle-to-Vehicle (V2V) communication, integrating federated learning, blockchain, and edge computing, as illustrated in Figure 1.

Consider each vehicle V_i equipped with an On-Board Unit and local IDS, where anomaly detection is computed using

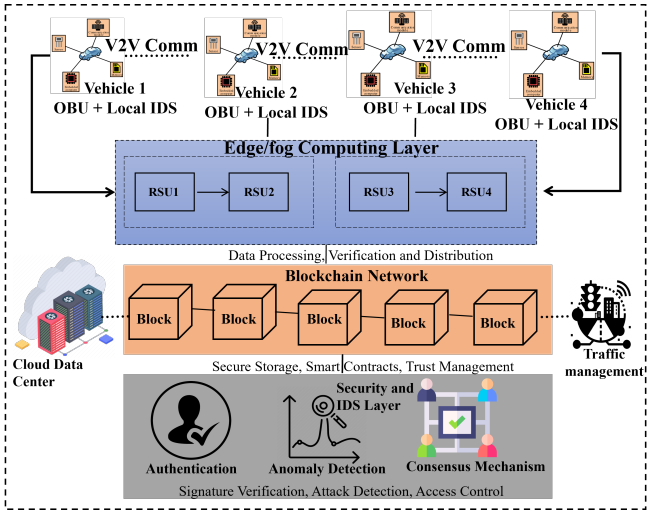

Fig. 1. Blockchain-enabled V2V security architecture with federated learning and IDS integration.

a Multi-layer Perceptron (MLP) to analyze extracted feature vectors $\phi(D_i)$, as in Equation 1.

$$\mathcal{F}_{\text{MLP}}(\phi(D_i)) = \text{Softmax}(W_3 \cdot \sigma(W_2 \cdot \sigma(W_1 \cdot \phi(D_i) + b_1) + b_2) + b_3). \tag{1}$$

Each roadside unit (RSU) maintains a local model $\mathcal{M}_i$, updated with local data D_i using gradient descent $\mathcal{M}_i^{new} = \mathcal{M}_i - \eta \nabla \mathcal{L}(\mathcal{M}_i, D_i)$. The global model $\mathcal{M}_{global}$ is updated by averaging the local models in Equation 2.

$$\mathcal{M}_{global}^{new} = \frac{1}{N} \sum_{i=1}^{N} \mathcal{M}_i^{new}. \tag{2}$$

Model updates and alerts are recorded on the PureChain, ensuring integrity. Each block b_t contains data, a timestamp, the previous block's hash, and proof of PoA^2 $b_t = (\text{block\_data}, \text{timestamp}, \text{hash}_{b_{t-1}}, \text{proof})$. The security layer includes authentication Auth_i, federated anomaly detection $\mathcal{A}_i$, and the PoA^2 consensus mechanism, uses a majority vote on model updates $C = \text{Majority}(V_1, V_2, \ldots, V_N)$. This model integrates federated learning, blockchain for data integrity, and PoA^2 for secure coordination, enabling scalable, privacy-preserving, and reliable updates.

III. Experimentation and Performance Analysis

We simulated the framework using 10, 20, and 30 federated clients over 100 communication rounds. Key metrics analyzed include model accuracy, latency, and throughput under different node densities. Figure 2 shows that the system maintains high accuracy across all configurations, with varying accuracy across different rounds and client configurations, reflecting the dynamic nature of vehicular edge computing systems in real-world scenarios. With 20 and 30 clients, the approach consistently exceeded 96% accuracy, demonstrating scalability and robustness under diverse vehicular data distributions. Figure 3 shows the performance tradeoff in a

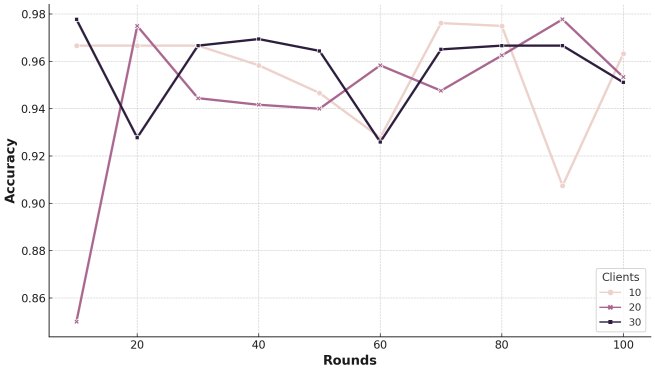

Fig. 2. Accuracy trends across rounds for different client counts.

blockchain-enabled vehicular edge computing system with varying client configurations. While increasing the number of clients improves throughput, it also raises latency. For 10 clients, latency remained below 0.1s/block with a throughput of 10 blocks/sec. Despite slight latency increases for higher client counts, the system maintained efficient consensus and throughput, demonstrating blockchain scalability.

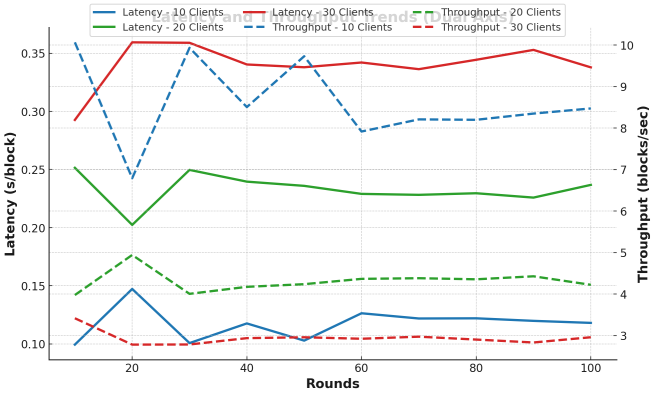

Fig. 3. Latency and throughput across client configurations.

The results confirm the system's performance in distributed vehicular environments, with a modular design that supports deployment across urban, highway, and rural areas. By eliminating central dependency and incorporating blockchain-backed accountability, our approach overcomes the limitations in [7]. The federated learning setup preserves privacy by not sharing local vehicular data directly, in line with [5]. The blockchain audit trail also enhances forensic traceability, improving system reliability post-attack.

IV. Conclusion and Future Work

This study proposed a blockchain-integrated, federated learning framework for secure V2V communication. Simulation results validate the approach regarding accuracy, latency, and throughput. Future directions include incorporating dynamic reputation scoring for misbehaving nodes, optimizing smart contract execution for energy efficiency, and validating the system on real vehicular datasets. Optimizing the system to balance throughput and latency, managing client loads, and improving the efficiency of blockchain operations are critical for ensuring system security and performance in large-scale vehicular networks.

Acknowledgment

This work was partly supported by the Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 33%) and by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 34%).

References

[1] X. Zhu, Z. Li, Y. Jiang, J. Xu, J. Wang, and X. Bai, "Real-Time Vehicle-to-Vehicle Communication-Based Network Cooperative Control System Through Distributed Database and Multimodal Perception: Demonstrated in Crossroads," in *International Congress on Information and Communication Technology*. Springer, 2024, pp. 133–146.

[2] L. He, F. Li, H. Xu, W. Xia, X. Zhang, and X. Tao, "Blockchain-Based Vehicular Edge Computing Networks: The Communication Perspective," *Science China Information Sciences*, vol. 66, no. 7, p. 172301, 2023.

[3] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Homomorphic encryption for privacy-preserving misbehavior detection in the internet of vehicles," in *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2025, pp. 0320–0324.

[4] P. Surapaneni, S. Bojjagani, V. C. Bharathi, M. Kumar Morampudi, A. Kumar Maurya, and M. Khurram Khan, "A Systematic Review on Blockchain-Enabled Internet of Vehicles (BIoV): Challenges, Defenses, and Future Research Directions," *IEEE Access*, vol. 12, pp. 123 529–123 560, 2024.

[5] H. L. Nakayiza, L. A. Chijioke Ahakonye, D.-S. Kim, and J. M. Lee, "Resource-Aware Adaptive Federated Learning for Enhanced DDoS Detection in Vehicular Ad Hoc Networks," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*, 2024, pp. 1262–1267.

[6] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[7] I. Ullah, X. Deng, X. Pei, H. Mushtaq, and Z. Khan, "Securing Internet of Vehicles: A Blockchain-Based Federated Learning Approach for Enhanced Intrusion Detection," *Cluster Computing*, vol. 28, no. 4, p. 256, 2025.

[8] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025.

[9] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular Edge Computing and Networking: A Survey," *Mobile networks and applications*, vol. 26, pp. 1145–1168, 2021.