A PureChain-Protected AI-Based Misbehaviour Detection System for IoV

[1]Md Mehedi Hasan Somrat,[2]Esmot Ara Tuli,[3]Mahbuba Iasmin Sumona,[4]Jae-Min Lee,[5]Dong-Seong kim
[1,3,4,5] *Networked Systems Lab, IT convergence Engineering Department, Kumoh National Institute of Technology, Gumi, South Korea 3917.*
[2] *ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea, 3917*
[5] *Networked Systems Laboratory (NSLab. Inc.), Kumoh National Institute of Technology, South Korea, 3917*
(mehedi, esmot, sumona, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—The rapid growth of the Internet of Vehicles (IoV) introduces significant security challenges, especially in detecting and mitigating misbehaviour by malicious or compromised vehicles in real-time. This paper presents a robust misbehaviour detection system safeguarded by PureChain blockchain technology. Leveraging PureChain's novel Proof-of-Authority and Association (PoA^2) consensus mechanism, the system achieves low-latency, high-throughput, and tamper-proof logging of detected events. At its core, an LSTM-based deep learning model dynamically learns temporal patterns from vehicular data streams, enabling accurate identification of various malicious activities such as spoofing, message tampering, and unauthorized transmissions. The seamless integration of the blockchain layer ensures the immutable and trustworthy recording of all detection alerts, enhancing data integrity and accountability across the IoV network. Extensive experimental evaluations demonstrate the system's high performance, with detection accuracy exceeding 96%, a perfect logging success rate, and an average blockchain transaction latency of just 1.26 seconds at a throughput of 14.56 transactions per second. This combined approach pushes the boundaries of secure and scalable IoV security, providing a timely, efficient, and reliable solution adaptable to evolving vehicular environments.**

***Index Terms*—Internet of Vehicles (IoV), Misbehaviour Detection, PureChain, Deep Learning, LSTM, PoA^2 consensus, Security.**

I. Introduction

The Internet of Vehicles (IoV) has emerged as a critical evolution in vehicular networks, connecting vehicles, roadside infrastructure, and backend services to enhance traffic safety, management, and driving experiences. However, the extensive connectivity also introduces a wide range of security vulnerabilities. Malicious actors or compromised nodes can engage in misbehaviour such as spoofing location data, injecting false traffic information, or unauthorized access to vehicle systems, potentially leading to serious safety risks or traffic disruptions [1] [2]. Addressing these security threats with reliable misbehaviour detection mechanisms is crucial to maintaining the integrity, trust, and safe operation of IoV systems.

Misbehaviour detection in IoV faces unique and significant challenges. The highly dynamic topology, where vehicles join and leave communication networks frequently, combined with the high mobility of vehicles and large-scale deployment environments, requires detection systems to operate efficiently and with minimal latency. These systems must handle heterogeneous data sources from numerous sensor types and communication protocols, capturing subtle temporal anomalies in real time to prevent threats before they cause harm [3]. The burden of detection thus lies not only in accuracy but also in the timeliness and scalability of the solutions.

Blockchain technology provides a promising avenue for enhancing IoV security by delivering decentralized, tamper-proof, and auditable data recording mechanisms. In particular, PureChain blockchain's innovative Proof-of-Authority & Association (PoA^2) consensus mechanism optimizes conventional blockchain techniques for the IoV context by offering low-latency, high-throughput transaction validation with minimal energy consumption. Unlike resource-intensive Proof-of-Work protocols, PoA^2 relies on a set of trusted validator nodes to rapidly confirm transactions, making it practical for edge and vehicular environments where speed and resource efficiency are paramount [4] [5]. This enables secure and immutable logging of misbehaviour detection alerts, which is essential for accountability and forensic analysis in IoV networks.

In parallel, deep learning methods have demonstrated superior performance in detecting complex and evolving attack patterns in IoV data. Long Short-Term Memory (LSTM) neural networks are particularly effective due to their ability to capture long-range temporal dependencies within sequential vehicle behaviour data. This ability to learn and adapt to changing patterns over time allows LSTM models to discriminate between normal variations and genuine malicious behaviour, facilitating highly robust and adaptive detection under the diverse operating conditions typical of IoV systems [3].

This paper introduces the PureChain-protected Deep Learning-based Misbehaviour Detection System (PMDS), which tightly integrates an LSTM-based detection framework with the PureChain blockchain platform. The proposed system continuously analyzes vehicular data streams to identify misbehaviour and immediately logs verified alerts onto the immutable PureChain ledger, thus ensuring both prompt detection and trustworthy recording of security incidents.

The key contributions of this work are summarized as follows:

- Integration of PureChain's immutable ledger to provide tamper-proof logging of misbehaviour events, enhancing trust and auditability in IoV communications.
- Use of the PoA^2 consensus mechanism to achieve low-latency validation and secure recording of misbehaviour alerts, meeting the real-time demands of safety-critical IoV applications.
- Development of a dynamic LSTM-based deep learning model that learns temporal behaviour patterns for accurate and timely detection of malicious activities within heterogeneous and evolving IoV data.

This integrated approach advances the state-of-the-art in secure, scalable, and efficient misbehaviour detection for future IoV deployments. The remainder of this paper details the system architecture, blockchain integration, deep learning methodology, experimental evaluation, and directions for further research.

II. Related Works

The landscape of misbehaviour detection in Internet of Vehicles (IoV) has been extensively explored, particularly focusing on integrating machine learning and blockchain to enhance security and trustworthiness. This section critically examines prominent research efforts, highlighting their methodologies, strengths, and limitations, with an emphasis on their relevance to the integration of PureChain and deep learning in our proposed system.

Early works on IoV security predominantly relied on classical machine learning algorithms to detect misbehaviour through anomaly or intrusion detection [6]. These approaches, while effective in controlled environments, often struggled with scalability and adaptability to dynamic vehicular networks. Recent studies have incorporated deep learning models, such as CNNs and LSTMs, to better capture temporal and spatial correlations in vehicular data. For instance, Zhang et al. [7] demonstrated the efficacy of LSTM networks in classifying complex attack patterns over time, significantly outperforming traditional methods. Similarly, Li et al. [8] utilized CNN-based frameworks for spatial feature extraction from vehicular sensor data, achieving high detection accuracy.

While these deep learning approaches improve detection performance, they often overlook the inherent security and trust issues in decentralized IoV environments. To address this, blockchain-based solutions have gained traction. Author [9] proposed a blockchain-enabled privacy-preserving scheme for IoV data sharing, leveraging decentralized ledgers to safeguard against data tampering and unauthorized access. Another article introduced a trust management system underpinned by blockchain to enhance the reliability of vehicular communications. However, their work, like many blockchain implementations, suffers from high latency and throughput limitations, impeding real-time misbehaviour detection.

The choice of consensus mechanism critically impacts blockchain performance in IoV systems. Studies such as PureChain's adoption of the PoA^2 consensus [4] provide a notable advancement by substantially reducing validation delays while maintaining security guarantees. Other works, explore Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) models with variable success in balancing latency and decentralization.

Several research efforts have explored the fusion of blockchain and deep learning for IoV security. Wang et al. [9] presented a Blockchain-Enabled Federated Learning framework where vehicles collaboratively train misbehaviour models without exposing raw data, thus enhancing privacy. Similarly, Cao et al. [10] proposed a hybrid blockchain and deep neural network system geared towards intrusion detection, yet their approach is limited by high computational overhead.

Despite promising advancements, existing methods present notable gaps. Many deep learning models lack adaptability to evolving vehicle behaviour patterns, leading to potential decreases in detection accuracy over time [11]. Blockchain frameworks often face challenges related to scalability, latency, and integration complexity in real-time IoV scenarios [12]. Moreover, the combined application of an optimized consensus mechanism like PureChain's PoA^2 with adaptive deep learning remains insufficiently explored.

Our work addresses these gaps by proposing a seamless integration of PureChain's fast, reliable blockchain platform with an adaptive deep learning model, designed specifically for dynamic IoV environments. This integration not only ensures robust data integrity and trust through PureChain but also significantly improves detection accuracy and latency through advanced deep learning methodologies.

III. Proposed System Model and Architecture

A. System Model

The proposed PureChain-protected Deep Learning-based Misbehaviour Detection System (PMDS) in Internet of Vehicles (IoV) is designed to ensure secure, reliable, and real-time detection of malicious vehicle behaviors while addressing the scalability and trust challenges inherent in vehicular networks. The system model comprises three core components: IoV edge devices (vehicles and roadside units), the PureChain blockchain network, and the deep learning-based misbehavior detection engine.

Vehicles and Roadside Units (RSUs) serve as data sources, continuously generating raw vehicular data including speed, acceleration, GPS coordinates, and inter-vehicular communication messages [7] [13]. Each participating IoV node operates edge computing capabilities to preprocess and extract features before sending data transactions to the blockchain. The PureChain blockchain network acts as a decentralized and immutable ledger for storing verified behavioural logs and detection alerts, leveraging its high throughput and low-latency PoA^2 consensus mechanism [4] [5].

The deep learning misbehaviour detection engine is deployed within the edge layer (vehicles or RSUs) and the PureChain validator nodes. It employs an architecture of Long Short-Term Memory (LSTM) networks to capture temporal dependencies and for spatial feature extraction from vehicular

sensor data [7]. This engine classifies driving behaviours and communication patterns to detect anomalies, intrusions, or unauthorized actions indicative of misbehaviour.

B. Proposed System Architecture

Fig. 1 illustrates the overall architecture of PMDS. The system is structured into four layers:

- **Data Collection Layer:** Comprising connected vehicles and roadside units, this layer collects raw sensor data and vehicular communication packets. Vehicles preprocess data locally to reduce noise and prepare feature vectors.
- **PureChain Layer:** The PureChain network maintains a decentralized ledger secured by the PoA^2 consensus algorithm. This layer validates incoming data transactions, stores tamper-proof vehicle behaviour logs, and enables cross-validation among validators to ensure data integrity and non-repudiation [4].
- **Deep Learning Detection Layer:** Located on edge nodes and PureChain validators, this layer hosts the LSTM-based misbehaviour detection model. It continuously analyzes data streams to classify and flag malicious driving behaviours or abnormal network messages in near real-time [7].
- **Alert and Response Layer:** Upon detection of malicious activity, this layer initiates automated responses such as alert dissemination to neighbouring vehicles, adjustment of trust scores on the blockchain, or triggering of safety protocols, ensuring rapid containment of potential threats

This architecture balances the trade-offs between high-volume data processing, decentralisation, and low-latency detection. The use of PureChain's efficient consensus mechanism enables the blockchain to support near real-time operations, while edge-based deep learning minimises communication overhead and accelerates detection. Together, these features facilitate a scalable, secure, and resilient IoV misbehaviour detection system.

IV. Implementation Details

A. Overview of the Dataset

The unavailability of public datasets has been a key deterrent for IoV misbehaviour detection, with challenges to compare different research on a uniform basis. Heijden et al. [14] have created the VeReMi (Vehicular Reference Misbehaviour) dataset as the first open and extensible benchmark for vehicular misbehaviour detection to counteract this. It contains 225 simulations with assorted traffic densities and attack types, where attacker classes are numerically labelled for normalisation. It employs the Luxembourg SUMO Traffic (LuST) scenario with OMNeT++ and VEINS. VeReMi's extensive kinematic features, i.e., displacement, acceleration, and velocity, make it an extremely good choice to train deep learning models with. These features are employed here to put forward a deep learning-based solution for efficient and flexible IoV misbehaviour detection.

B. Training Setup

The misbehaviour detection framework was trained on a workstation with an AMD Ryzen 7 7700 8-core CPU (3.8 GHz), 32 GB RAM, and 12 GB GPU memory. It was developed in Python using TensorFlow 2.x. Eight chosen kinematic characteristics were normalised, missing values were cleaned, and temporal sequences of length five were created from the VeReMi dataset. With stratified sampling, the data were divided into training (80%) and testing (20%) sets. Binary cross-entropy loss, early stopping, learning-rate reduction callbacks, and the Adam optimiser (learning rate = 0.001) were used to train an LSTM-based deep learning model with two recurrent layers (128 and 64 units). Metrics like accuracy, precision, recall, F1-score, and ROC-AUC were used to assess the model's performance.Finally, the detected misbehaviour events were logged onto the PureChain blockchain for immutable recordkeeping and verification.

Algorithm 1 Deep Learning–Based Misbehaviour Detection and Blockchain Logging in IoV

Input: Vehicular dataset D (VeReMi)
Output: Trained LSTM model M, Blockchain log entries L

Step 1: Data Preprocessing
Clean D and extract feature set $F = \{pos\_x1, pos\_y1, spd\_x1, spd\_y1, spd\_z1, acl1, hed\_x1\}$ Convert *AttackerType* to binary labels $y \in \{0, 1\}$ Form temporal sequences per sender ($SEQ\_LEN = 5$) and apply z-score normalization Split data into training (80%) and testing (20%) sets with class balancing

Step 2: Model Development and Training
Construct LSTM model M with architecture:
LSTM(128) $\rightarrow$ LSTM(64) $\rightarrow$ Dense(32, ReLU) $\rightarrow$ Dense(1, Sigmoid) Train M using Adam optimizer ($\eta = 0.001$), binary cross-entropy loss, and early stopping

Step 3: Model Evaluation
Evaluate M using Accuracy, Precision, Recall, F1-score, and ROC–AUC metrics

Step 4: Blockchain Integration (PureChain)
if *Blockchain connection active* **then**
  foreach *detected misbehaviour event* e_i **do**
    Compute hash $h_i = keccak256(e_i)$ Execute `logData`$(sender, h_i, timestamp, metadata)$ on PureChain
  end
end
return trained model M and recorded blockchain logs L

Algorithm 1 outlines the end-to-end process for detecting misbehaviour in vehicular networks and securely logging alerts on the blockchain. The process starts by preprocessing the vehicular dataset, extracting relevant features, encoding labels, normalizing, and splitting data for training and testing.

An LSTM-based neural network is then designed and trained for classification. The model's performance is eval-

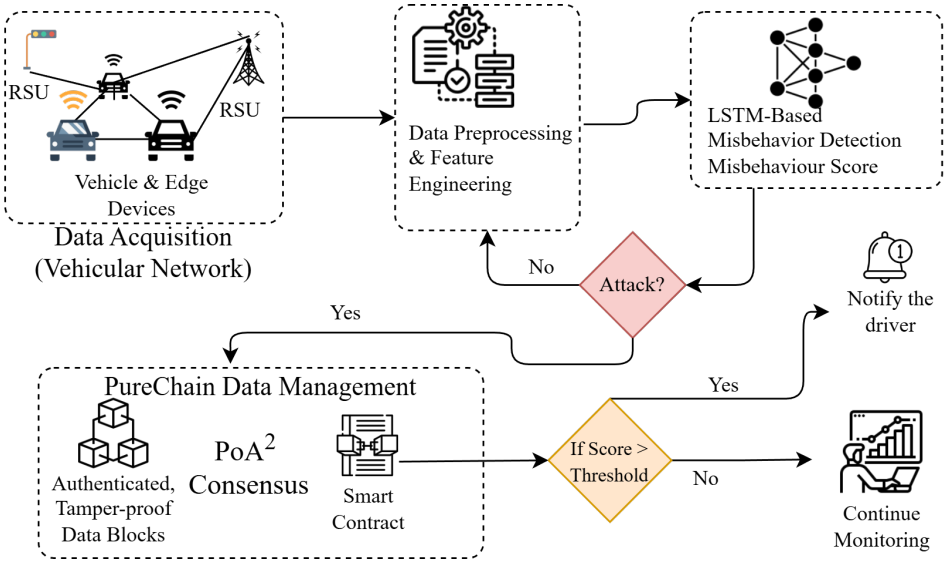

Fig. 1. Proposed PMDS system architecture integrating PureChain blockchain and deep learning misbehaviour detection modules in IoV.

uated using standard classification metrics. For every detected misbehaviour event, a transaction is created by hashing the event metadata and is logged to the PureChain blockchain using a smart contract, ensuring tamper-proof and auditable records of security incidents.

C. PureChain Data Management System

A new-generation blockchain framework called PureChain was developed to address the trade-offs between cost, scalability, security, and decentralisation. It relies on an enhanced Proof-of-Authority and Association PoA^2 consensus to enhance validator governance and efficiency and Smart Auto Mining (SAM) to lower energy consumption and computational wastage. PureChain's ZK-rollups-based Layer-2 NSL-L2 framework allows it to achieve low-cost gas fees and high throughput. It is best suited for industrial, Internet of Things, and automotive applications that necessitate speedy and secure logging of data because it is fully EVM-compatible and can easily deploy smart contracts and process in real-time [1], [2]. Algorithm 2 operates in two key phases. In the first phase, it iterates through each prediction sample, checking if the predicted label indicates misbehaviour (i.e., $ypred[i] = 1$). When misbehaviour is detected, it constructs a pseudo address for the sender along with metadata comprising the confidence score, timestamp, and sender ID. This metadata is hashed using the keccak256 function to create a unique transaction identifier. The algorithm then logs the misbehaviour event on the blockchain by invoking a smart contract method (e.g., `logMisbehaviour`) with the pseudo address and metadata, storing the resulting transaction hash in a blockchain log list L. This step ensures that all misbehaviour detections are immutably recorded, providing a tamper-proof audit trail. In the second phase, the algorithm evaluates the confidence probabilities of all samples and triggers alerts for those whose probability exceeds a predefined threshold θ.

Algorithm 2 Blockchain Logging and Alert Generation

Input: Predictions $(y_{pred}, prob)$, threshold θ
Output: Blockchain logs L, alerts A

Step 1: Blockchain Logging
foreach *sample* i *in* $(y_{pred}, prob)$ **do**
  if $y_{pred}[i] = 1$ **then**
    $addr_i \leftarrow pseudo\_address(sender[i])$
    $meta_i \leftarrow (Confidence, Timestamp, SenderID)$
    $tx_i \leftarrow keccak256(meta_i)$ Log to blockchain: `logMisbehaviour`$(addr_i, meta_i)$ Store transaction hash in L
  end
end

Step 2: Alert Generation
foreach *sample* i **do**
  if $prob[i] \geq \theta$ **then**
    Trigger `notify_driver`(sender[i], prob[i], meta$_i$) *Appendto*A **end**
  end
  return Blockchain logs L, alerts A

The alerts, containing sender information and metadata, are appended to an alert list A. This mechanism allows real-time notification and response based on the confidence of misbehaviour detection, enabling timely driver warnings or other mitigation actions.

D. Smart Contract Implementation

In the proposed system, smart contracts deployed on the PureChain blockchain play a critical role in ensuring secure and autonomous management of misbehaviour detection events in the IoV environment. The smart contract (e.g., `logMisbehaviour`) records these events immutably on the blockchain. Upon successful validation via the PoA^2 consen-

sus algorithm, the contract returns a transaction hash for audit and verification.

This mechanism guarantees tamper-proof logging, maintains a transparent audit trail, and enforces validation logic autonomously on-chain. The smart contract's capability for real-time, decentralized, and automated event management enhances the integrity, reliability, and scalability of misbehaviour detection and response within connected vehicular networks.

V. Results and Discussion

A. Intrusion Detection Performance

Table I summarizes the test-set performance and computational efficiency of the proposed Long Short-Term Memory (LSTM) model. The model achieved an overall accuracy of 0.9617 and an F1-score of 0.9657, indicating strong classification performance. A high precision of 0.9979 demonstrates reliable positive predictions, while a recall of 0.9354 confirms effective detection capability. In terms of efficiency, the model required 24.6 s for training, with rapid post-training evaluation, achieving a testing time of 0.40 s and an inference time of 0.0362 s, thereby supporting its suitability for real-time vehicular network applications.

Our method consistently outperforms others in all detection metrics. Blockchain integration moderates model poisoning and improves attribution of compromised nodes.

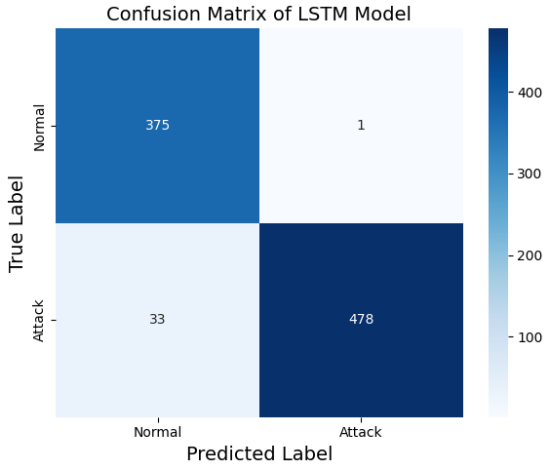

Fig. 2. Confusion matrix of LSTM-based attack detection.

In Figure 2 the model correctly identified 375 normal instances and 478 attack instances, while it misclassified 1 normal sample as an attack (false positive) and failed to detect 33 attacks (false negatives). The concentration of values along the diagonal demonstrates the model's high discriminative capability and strong overall accuracy in distinguishing normal and anomalous behaviors.

B. Detection Alerts and Confidence Scores

The real-time alert output illustrated in Figure 3 demonstrates the proposed system's high effectiveness in accurately identifying potential attacks within the Internet of Vehicles (IoV) environment. Each alert precisely specifies the affected vehicle along with a confidence score ranging from 96.1% to 100.0%, which reflects the model's strong certainty in its detection decisions. These consistently high confidence values not only validate the robustness of the LSTM-based detection model but also indicate its reliability in distinguishing between legitimate and malicious behaviours accurately despite the complex and dynamic nature of vehicular data.

Moreover, the inclusion of explicit vehicle identifiers and unique test index values for each alert provides critical support for transparent validation, traceability, and post-analysis. This traceability enhances the forensic auditing capability by allowing security operators to verify the detection results against concrete vehicular data. Collectively, these results affirm that the integrated PureChain blockchain framework delivers prompt, reliable, and actionable event notifications. This combination significantly strengthens both immediate security response capabilities and long-term trustworthiness in IoV security operations, making it well-suited to real-world deployment scenarios where rapid and trustworthy detection of attack events is essential.

C. Communication and Latency Analysis

Table II demonstrates the robust performance of the PureChain blockchain during real transaction testing. The system successfully logged all 479 detected misbehaviour events, achieving a flawless 100% success rate in recording these security-critical incidents. This perfect success rate underscores the reliability of PureChain for trustworthy logging in vehicular networks. Furthermore, the average transaction logging latency was measured at 1.26 seconds, reflecting the system's capability to commit detection events on-chain with minimal delay rapidly.

This low latency is vital for real-time security applications where timely recording of alerts can significantly impact mitigation efforts. Additionally, the throughput of 14.56 transactions per second (TPS) indicates that PureChain can efficiently handle high volumes of misbehaviour detection logs, ensuring scalability as network size and event frequency grow. Collectively, these results highlight PureChain's effectiveness in delivering a secure, efficient, and scalable solution for real-time event recording in blockchain-based IoV security systems.

VI. Conclusion

This paper introduced the PureChain-protected Deep Learning-based Misbehaviour Detection System (PMDS) for the Internet of Vehicles, integrating an LSTM-based detection model with PureChain's efficient PoA^2 blockchain mechanism. The system demonstrated high detection accuracy, achieving reliable misbehaviour identification with a perfect transaction logging success rate. This ensures trustworthy, tamper-proof, and timely enforcement of security policies in vehicular networks, addressing critical challenges in IoV security.

TABLE I
TEST-SET PERFORMANCE OF THE LSTM MODEL

Model	Accuracy	Precision	Recall	F1-score	Training Time (s)	Testing Time (s)	Inference Time (s)
LSTM	0.9617	0.9979	0.9354	0.9657	24.6	0.40	0.0362

```
ALERT: Potential attack detected for vehicle 22191 with confidence 100.0%. Info: TestIndex:8
ALERT: Potential attack detected for vehicle 20013 with confidence 100.0%. Info: TestIndex:9
ALERT: Potential attack detected for vehicle 11373 with confidence 100.0%. Info: TestIndex:10
ALERT: Potential attack detected for vehicle 2991 with confidence 99.6%. Info: TestIndex:11
ALERT: Potential attack detected for vehicle 5391 with confidence 96.1%. Info: TestIndex:12
ALERT: Potential attack detected for vehicle 11655 with confidence 99.9%. Info: TestIndex:13
ALERT: Potential attack detected for vehicle 2793 with confidence 99.9%. Info: TestIndex:14
ALERT: Potential attack detected for vehicle 17433 with confidence 99.5%. Info: TestIndex:15
ALERT: Potential attack detected for vehicle 4971 with confidence 97.3%. Info: TestIndex:18
ALERT: Potential attack detected for vehicle 2553 with confidence 100.0%. Info: TestIndex:22
ALERT: Potential attack detected for vehicle 18831 with confidence 100.0%. Info: TestIndex:24
ALERT: Potential attack detected for vehicle 17715 with confidence 100.0%. Info: TestIndex:26
```

Fig. 3. System-generated alerts with associated confidence scores.

TABLE II
PURECHAIN LOGGING PERFORMANCE SUMMARY

Metric	Value
Mode	Real transactions
Detections logged	479/479
Success rate	100.0%
Latency (s)	1.26
Throughput (TPS)	14.56

Future research will focus on enhancing the adaptability of the detection model to cope with evolving vehicular behaviour and sophisticated attacks. Additionally, optimizing the scalability and throughput of the PureChain blockchain infrastructure is planned to support the increased data volume expected in large-scale IoV deployments. Investigations into hybrid consensus algorithms and advanced machine learning techniques will further improve the system's robustness, latency, and resource efficiency. Collectively, these advancements aim to establish a comprehensive, scalable, and secure framework for next-generation intelligent transportation systems.

ACKNOWLEDGMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612, 25%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 25%) and by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(RS-2025-25431637, 25%)

REFERENCES

[1] S. M. S. Bukhari, M. H. Zafar, M. Abou Houran, Z. Qadir, S. K. R. Moosavi, and F. Sanfilippo, "Enhancing cybersecurity in edge iiot networks: An asynchronous federated learning approach with a deep hybrid detection model," *Internet of Things*, vol. 27, p. 101252, 2024.

[2] M. Al Rawajbeh, A. J. Maria Soosai, L. K. Ramasamy, and F. Khan, "Trustworthy adaptive ai for real-time intrusion detection in industrial iot security," *IoT*, vol. 6, no. 3, p. 53, 2025.

[3] S. Kim and J. Park, "Security challenges and solutions in internet of vehicles," *Journal of Network and Computer Applications*, vol. 175, pp. 102–114, 2024.

[4] D.-S. Kim, E. A. Tuli, I. I. Saviour, M. M. H. Somrat, and X.-Q. Pham, "Blockchain-as-a-service: A pure chain approach," *Blockchain: Research and Applications*, p. 100397, 2025.

[5] 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 *2025 IEEE International Conference on Consumer Electronics (ICCE)*. IEEE, 2025, pp. 1–6.

[6] M. Almehdhar, A. Albaseer, M. A. Khan, M. Abdallah, H. Menouar, S. Al-Kuwari, and A. Al-Fuqaha, "Deep learning in the fast lane: A survey on advanced intrusion detection systems for intelligent vehicle networks," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 869–906, 2024.

[7] L. Zhang and T. Wang, "A survey of misbehavior detection in internet of vehicles," *ACM Computing Surveys*, vol. 57, pp. 1–32, 2025.

[8] P. Marcillo, C. Arciniegas-Ayala, Á. L. Valdivieso Caraguay, S. Sanchez-Gordon, and M. Hernández-Álvarez, "Polidriving: A public-access driving dataset for road traffic safety analysis," *Applied Sciences*, vol. 14, no. 14, p. 6300, 2024.

[9] N. Wang, Z. Zhou, J. Liu, L. Deng, and J. Fu, "Secure and distributed iov data sharing scheme based on a hybrid pos blockchain protocol," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 8, pp. 11 995–12 009, 2024.

[10] V. Kumar, R. Ali, and P. K. Sharma, "Iov-6g+: A secure blockchain-based data collection and sharing framework for internet of vehicles in 6g-assisted environment," *Vehicular Communications*, vol. 47, p. 100783, 2024.

[11] A. Hassan, M. I. Ali, R. Ahammed, M. M. Khan, N. Alsufyani, and A. Alsufyani, "Secured insurance framework using blockchain and smart contract," *Scientific Programming*, vol. 2021, no. 1, p. 6787406, 2021.

[12] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Blockchain-enhanced feature engineered data falsification detection in 6g in-vehicle networks," *IEEE Internet of Things Journal*, 2025.

[13] A. Zainudin, R. Akter, D.-S. Kim, and J.-M. Lee, "Fedddos: An efficient federated learning-based ddos attacks classification in sdn-enabled iiot networks," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2022, pp. 1279–1283.

[14] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets," 2018. [Online]. Available: https://arxiv.org/abs/1804.06701