Blockchain-Enhanced Feature Engineered Data Falsification Detection in 6G In-Vehicle Networks

Hope Leticia Nakayiza, Love Allen Chijioke Ahakonye, *Member, IEEE*, Dong-Seong Kim, *Senior Member, IEEE*, and Jae-Min Lee, *Member, IEEE*

***Abstract*—Increased automation, connectivity, and data sharing enabled by 6G technology have heightened the vulnerability of Internet of Vehicles (IoV) networks. Addressing this challenge requires an intrusion detection system (IDS) capable of accurately identifying data falsification within IoV while adhering to real-time constraints. This article presents a Blockchain-enhanced feature-engineered IDS to ensure precise attack detection and classification with minimal computational overhead in in-vehicle networks (IVNs). The proposed lightweight IDS utilizes a hybrid Pearson's Correlation Coefficient (PCC) feature selection technique designed for deployment on the Telematics Control Unit (TCU). Furthermore, we propose a custom private blockchain network utilizing the proof of authority and association (PoA^2) consensus mechanism, deployable on the roadside unit (RSU), for the secure logging of vehicle electronic control unit (ECU) information, detection results, and the automatic isolation of malicious ECUs via smart contracts. Experimentation analysis demonstrates that the proposed approach achieves notable performance, with a 99.9% detection accuracy and minimal computation times of 0.24 and 1.32 s on the CICIoV2024 and CAN-Intrusion datasets. Furthermore, the system achieves high blockchain scalability, maintaining stable throughput of 16 tx/s and low transaction latency of 0.062 s under increasing ECU density and RSU coverage.**

***Index Terms*—6G IoV, blockchain, data falsification, feature engineering, intrusion detection system (IDS), in-vehicle networks (IVNs).**

I. Introduction

THE 5G networks have transformed communication efficiency, enabling diverse applications and laying a robust foundation for the 6G network paradigm [1] in the Internet of Vehicles (IoV). Projected for widespread adoption beyond 2030, 6G promises ultrareliable low-latency communication (URLLC), terahertz frequencies, and multiaccess edge computing (MEC) [1], thereby creating intelligent networks capable of real-time data generation, processing, and analysis [2] (see white paper on 6G Vision and Candidate Technologies[1];viewed July 10, 2024).

The interconnectedness in IoV enables seamless communication among vehicles, smart urban infrastructure, and other entities to support intelligent transportation systems [3], expected to evolve due to the capabilities of 6G. This architecture leverages vehicle-to-everything (V2X) communication, including vehicle-to-vehicle (V2V), infrastructure-to-vehicle or vehicle-to-infrastructure (I2V/V2I), vehicle-to-pedestrian (V2P), and vehicle-to-network (V2N) communication [3]. Reliable and secure V2X communication, standardized by the SAE J2735 [4] with basic safety messages (BSMs) transmitted at 100 ms intervals across 300–1000 m ranges [5], is integral to these critical advancements. Central to the IoV framework, in-vehicle networks (IVNs) connect onboard units (OBUs), sensors, actuators, and electronic control units (ECUs) via the controller area network (CAN) Bus protocol [6]. Roadside units (RSUs) and edge servers facilitate low-latency V2I communication and real-time processing for applications like threat detection [7]. The centralized cloud infrastructure supports large-scale data storage, analytics, and coordination across the IoV network, while 6G-enabled V2X protocols, such as Cellular V2X (C-V2X) and dedicated short-range communication (DSRC), ensure high-speed, reliable data exchange between components [7].

As vehicles increasingly become autonomous and interconnected, the volume and complexity of generated in-vehicle data grow exponentially, exposing CAN Bus vulnerabilities. Lacking authentication and encryption [8], the CAN Bus is susceptible to spoofing, denial of service (DoS), and data falsification attacks [9], where malicious entities manipulate sensor data or ECU commands, potentially leading to erroneous decisions and accidents [10]. In the broader 6G IoV ecosystem, threats extend beyond the vehicle to V2X layers encompassing the external, communication, infrastructure, and cloud layers. These threats, including jamming, eavesdropping, man-in-the-middle (MitM) attacks,and malware injections [11] exploit specific

Received 28 March 2025; revised 30 April 2025; accepted 9 May 2025. Date of publication 14 May 2025; date of current version 25 July 2025. This work was supported in part by the Innovative Human Resource Development for Local Intellectualization Program through the IITP Grant funded by the Korea Government (MSIT) under Grant IITP-2025-RS-2020-II201612 (25%); in part by the Priority Research Centers Program through the NRF funded by the MEST under Grant 2018R1A6A1A03024003 (25%); in part by the MSIT, South Korea, through the ITRC Support Program under Grant IITP-2025-RS-2024-00438430 (25%); and in part by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-ICT Challenge and Advanced Network of HRD (ICAN) Grant funded by the Korea Government (Ministry of Science and ICT) under Grant IITP-2025-2022-00156394* (25%). *(Corresponding author: Jae-Min Lee.)*

Hope Leticia Nakayiza, Dong-Seong Kim, and Jae-Min Lee are with the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: hopeleticia@kumoh.ac.kr; dskim@kumoh.ac.kr; ljmpaul@kumoh.ac.kr).

Love Allen Chijioke Ahakonye is with the ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi 39177, South Korea (e-mail: loveahakonye@kumoh.ac.kr).

Digital Object Identifier 10.1109/JIOT.2025.3569845

[1]http://www.caict.ac.cn/english/news/202106/P020210608349616163475.pdf

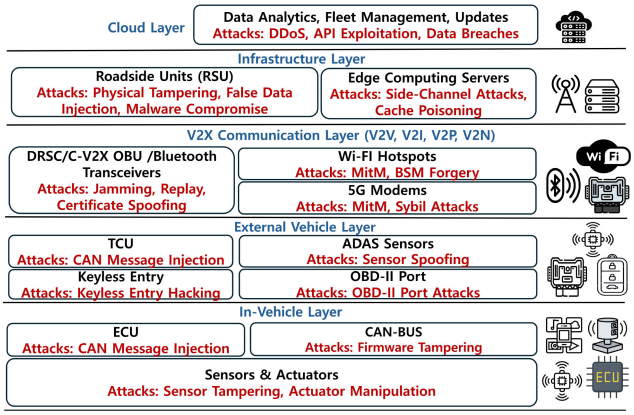


Fig. 1. Possible attacks across different layers of the IoV architecture.

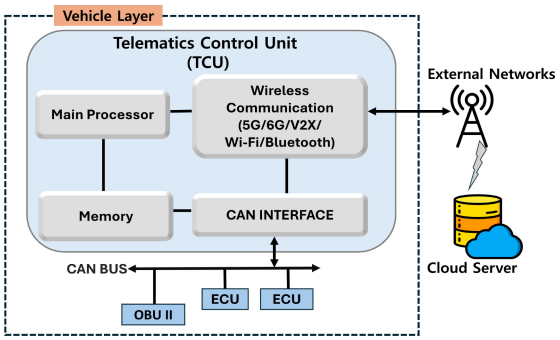


Fig. 2. Illustration of the TCU connecting the IVN to external networks via wireless communication technologies.

vulnerabilities across the IoV architecture, as depicted in Fig. 1.

The CAN Bus operates at relatively low speeds (typically 1 Mb/s) [8], constraining its ability to meet the high-throughput demands of external communication and blockchain integration in 6G IoV. To address this limitation, telematics control units (TCUs) serve as gateway ECUs to bridge internal and external vehicle networks [12], as shown in Fig. 2. Equipped with DSRCs and C-V2X modules, TCUs offer the processing power, security, and connectivity necessary for intrusion detection system (IDS) and blockchain operations, enabling real-time, low-latency data exchange between the CAN Bus and RSUs [11].

In 6G-based IVNs, extensive sensor and control unit data create high-dimensional datasets, causing delays and increased computational costs. Conventional IDS for IVNs face performance degradation in 6G-enabled IoV due to increased feature dimensions, making real-time, resilient threat detection challenging in dynamic, distributed topologies [13]. To mitigate this, feature engineering is applied to anomaly based IDS to boost ML model performance, thus improving data falsification detection while reducing computational costs [14]. An efficient IDS should accurately identify and extract relevant data while differentiating between malicious and normal traffic. Centralized approaches face single points of failure and latency, and local logging lacks tamper resistance and scalability. Blockchain addresses these issues by offering decentralized trust, immutable auditability, and automated

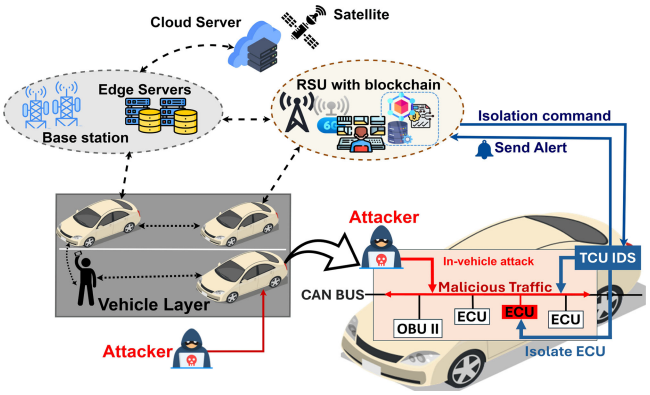


Fig. 3. Depiction of the IoV architecture showing the proposed in-vehicle IDS placement.

threat mitigation via smart contracts [15], [16], [17]. Despite significant efforts, detecting and mitigating in-vehicle threats such as data falsification and ECU misbehavior, remains challenging in 6G IVNs [18]. Existing studies primarily focus on deploying IDS on the CAN Bus, which restricts communication with advanced security mechanisms, such as blockchain, integrated into external network architectures. To address this gap, this study proposes a TCU-deployed IDS framework integrating feature-engineered ML with blockchain. Our contributions in this article are as follows.

1) Strategic deployment of the IDS on the TCU as a gateway ECU, addressing the architectural challenge of connecting IVNs to external security mechanisms without compromising the CAN Bus protocol.
2) A hybrid Pearson's Correlation Coefficient (PCC)-based feature selection (FS) approach combining PCC with partial correlation to identify the most significant features for attack detection with minimal redundancy, enhancing model interpretability while maintaining high accuracy.
3) A custom private blockchain network, PureChain, utilizing the Proof of Authority and Association (PoA^2) consensus mechanism for efficient, secure storage of vehicle ECU information and detection results.
4) Design of lightweight smart contracts for automated, real-time isolation of malicious nodes triggered by false message detection along the CAN bus protocol.

The system architecture in Fig. 3 illustrates the proposed placement of the IDS to ensure secure, decentralized communication while addressing the security demands of 6G IoV systems. By addressing CAN Bus vulnerabilities and V2X threats, this framework aims to deliver a scalable, secure solution for 6G IoV, advancing the safety and reliability of intelligent transportation systems.

II. Background Study and Related Works

This section reviews related works on IoV intrusion detection, feature engineering, and the implementation of blockchain to enhance security. Despite significant advancements, current solutions face limitations in scalability, real-time performance, and resilience against evolving threats.

A. In-Vehicle Intrusion Detection

Comprehensive studies on in-vehicle IDSs explore future trends and challenges, serving as a key reference for stakeholders. These studies review benchmark datasets, detection techniques, features, and attack types, detailing the development of AI-based in-vehicle IDSs, assessing AI model security, identifying limitations of current solutions, and proposing future research directions [19], [20], [21]. To enhance intrusion detection and classification accuracy within the 5G-V2X environment, Anbalagan et al. [22] introduced an advanced IDS that utilizes a modified deep convolutional neural network (DCNN). The study by [23] introduced a system for detecting false locations in IoV BSMs, utilizing an optimized Ensemble Random Forest to enhance security. Nakayiza et al. [24] evaluated various machine-learning algorithms to detect and classify data falsification introduced to the IVN via the CAN-Bus protocol. Furthermore, to analyze IVN traffic sequential patterns, Song et al. [25] introduced a DCNN-based IDS that effectively detected message injection attacks by monitoring alterations in CAN Bus traffic. While these approaches improve accuracy, they do not address data integrity and tamper resistance, which are crucial in ensuring trustworthy IDS logs and alerts.

B. Feature Engineering for Intrusion Detection

FS techniques, broadly classified into filter-based, wrapper-based, and embedded methods, play a pivotal role in optimizing ML models for intrusion detection [14]. Filter methods, characterized by their computational efficiency, excel with large datasets, whereas wrapper methods, though resource-intensive, enhance model accuracy through iterative optimization. Embedded approaches synergistically integrate the strengths of both, balancing efficiency and performance. This process is instrumental in anomaly detection, enabling the extraction of relevant features from raw data to identify patterns indicative of data falsification [26]. Within vehicular networks, feature engineering markedly elevates detection rates for attacks such as position falsification in VANETs [5], underscoring its relevance to in-vehicle security. By evaluating feature importance, we can gain deeper insights into data dynamics and model behavior, facilitating the prioritization of high-value features for predictive accuracy and advancing the interpretability of IDSs in 6G IoV networks. Abdelkreem et al. [5] and Anyanwu et al. [27] applied the PCC for FS on the VeReMi dataset, focusing on the association between BSM features and their corresponding classes. Additionally, Recursive Feature Elimination (RFE) to select the most useful features [28] and a stacked FS model for dimensionality reduction [29] were employed on the CAN-Intrusion and CICICDS2017 datasets. However, these approaches exhibit high execution times, posing challenges for real-time applications in 6G vehicular networks.

C. Blockchain in IoV Intrusion Detection

Blockchain has emerged as a promising solution for securing IoV by ensuring trust, data integrity, decentralized authentication mechanisms, and immutability [30]. Several studies have explored blockchain-enhanced IDS solutions. Ayaz et al. [31] suggested that strategic preemptive solutions can effectively implement these approaches, addressing IoT systems' evolving security and privacy needs. In their study, Salem et al. [32] employed a private blockchain network to enhance the protection and privacy of VANETs IVN. The centralized blockchain structure uses the central gateway. Su et al. [33] proposed a blockchain-based privacy protection system utilizing the Proof of Work consensus mechanism for secure user registration and two-way authentication in IoV. It addressed the central dependency issue inherent in traditional IoV systems. To improve security and automation within Industry 5.0, Anbalagan et al. [34] proposed a blockchain-assisted IDS to detect the various autonomous vehicle cyberattacks and provide a trusted 5G V2X network. Andreica et al. [35] developed an IDS for in-vehicle buses from which results were stored on the blockchain. To enhance vehicle privacy protection, Xie et al. [36] presented a distributed IDS combined with blockchain for intrusion results logging. Despite these advancements, existing blockchain-based IDS solutions present challenges such as high computational overhead, transaction latency, and scalability issues when integrated into real-time vehicular networks.

D. Summary of Related Studies

The integration of vehicle sensors and processing modules has surged due to automotive intelligence advancements [3]. These modules, typically connected via the CAN Bus and managed by ECUs, focus on maintaining consistent communication but often overlook node privacy protection. With vehicles evolving into mobile smart network terminals, ECUs are more exposed to increased security threats [37], [38]. While intrusion detection techniques and cryptographic defenses have been widely explored, existing solutions struggle with real-time constraints, leading to increased false positives and missed detections in dynamic IoV settings [5], [27], [28], [29]. Additionally, traditional IDS logging mechanisms lack tamper resistance, making them vulnerable to data manipulation. Table I provides a comparative analysis of existing studies, emphasizing the need for feature-engineered, blockchain-enhanced IDS frameworks to address the decentralized security requirements and real-time performance demands of 6G IoV networks.

III. System Model

This section introduces the proposed combination of feature engineering techniques with IDS using an optimized Decision Tree to detect data falsification and blockchain technology to securely store vehicle ECU information and detection results and isolate malicious ECUs. Fig. 4 is the system workflow of the proposed approach.

A. Blockchain Integration

A blockchain network was deployed on the RSU to secure vehicle ECU information and detection results and isolate malicious ECUs. The RSU acts as the control center, facilitating communication between vehicles and components. TCUs

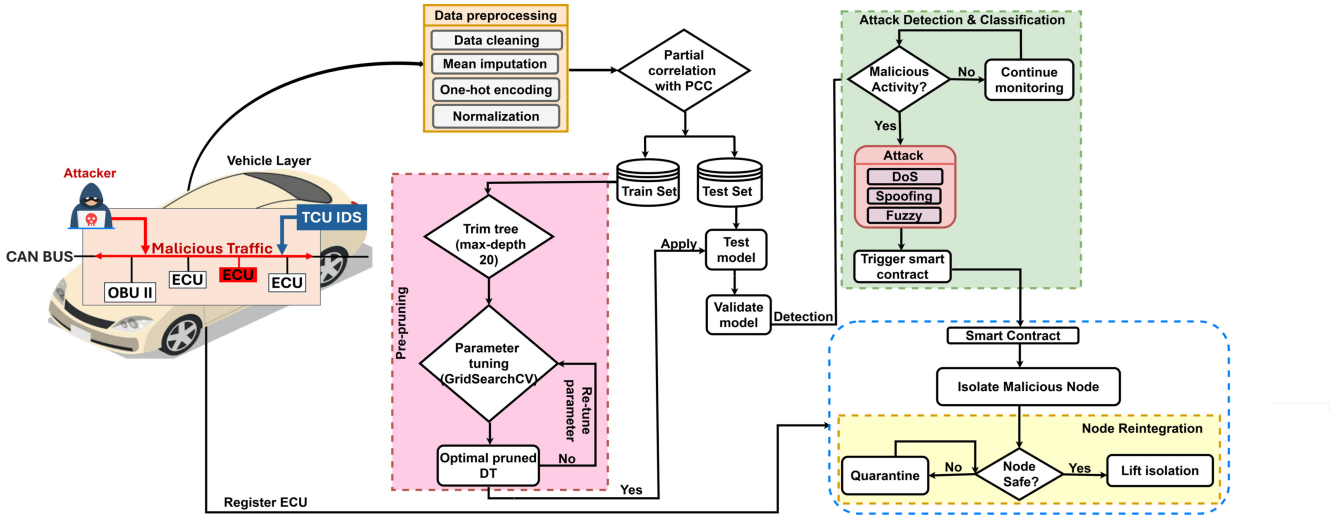


Fig. 4. Proposed blockchain-enhanced feature-engineered IDS workflow.

TABLE I
SUMMARY OF RELATED WORKS: COMPARATIVE ANALYSIS FOR OPTIMIZED INTRUSION DETECTION AND BLOCKCHAIN INTEGRATION IN IOV NETWORKS (✓: IMPLEMENTED/TIME BELOW 5 S, ✗: NOT IMPLEMENTED/TIME ABOVE 5 S)

Ref.	Dataset Used	FS	Execution Time <5s	Blockchain
[5]	VeReMi	✓	✗	✗
[22]	Simulated dataset	✗	✓	✗
[23]	VeReMi	✗	✗	✗
[25]	CAN-Intrusion	✗	✗	✗
[27]	VeReMi	✓	✗	✗
[28]	CICIDS2017, CAN-Intrusion	✓	✗	✗
[29]	CICIDS2017, CAN-Intrusion	✓	✗	✗
[34]	Simulated dataset	✗	✗	✓
[35]	CAN message data from 3 different vehicles	✗	✗	✓
[36]	UNSW_NB15 CAN Intrusion	✗	✗	✓
Proposed Approach	**CICIoV2024, CAN-Intrusion, BurST ADMA, CICDDoS2019, 5G-NIDD**	✓	✓	✓

serve as nodes, with the RSU as the master node to grant registration permissions and trigger smart contracts for isolating malicious nodes and logging security events. A custom private permissioned PureChain network [39], based on the proof of authority and association (PoA^2) consensus mechanism [39], was utilized. PoA^2 enhances security, efficiency, and reliability by using a standby validator [40]. In cases where validators become inactive, the network activates an idle redundant signer that identifies and replaces them to ensure uninterrupted network stability. This mechanism was chosen over others, like proof of stake or proof of work, for its lightweight nature and faster transaction times while maintaining robust security [41].

1) ECU Registration on the PureChain: The RSU registers ECUs using information such as vehicle ID, ECU ID, and ECU address to the blockchain network via the smart contract to allow their communication over the IVN. The RSU calls the function *registerECU*(*address*) for the address of the ECU to be passed as an argument. Upon calling this function, the RSU updates the *registeredECUs* list, marking the provided address as *true* to indicate that the ECU has been successfully registered as shown in Algorithm 1.

Algorithm 1: RSU Registers ECU

1: **procedure** REGISTERECU(*address*)
2: RSU calls *registerECU(address)*
3: *registeredECUs[address]* ← true
4: **end procedure**

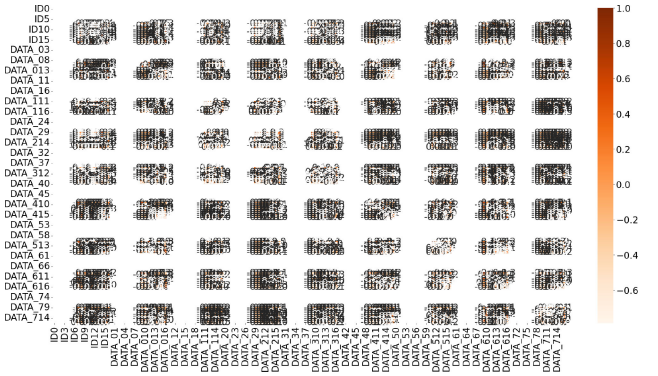


Fig. 5. CICIoV2024 dataset before preprocessing showing noisy, raw correlations across all features and the target class highlighting multicollinearity.

B. Data Preprocessing

The CICIoV2024 dataset [42],[2] comprising false messages that were injected via the CAN Bus protocol of a 2019 Ford Car containing all ECUs was leveraged for this study.

Fig. 5 is the raw heatmap for the CICIoV2024 dataset, showing noisy correlations and potential redundancy among features, which can obscure the direct relationship between individual features and the target attack types, highlighting the need for data preprocessing.

Managing missing values is crucial in data preprocessing. A common approach is mean imputation, which substitutes missing values with the dataset's average observed values. This

[2]https://www.unb.ca/cic/datasets/iov-dataset-2024.html

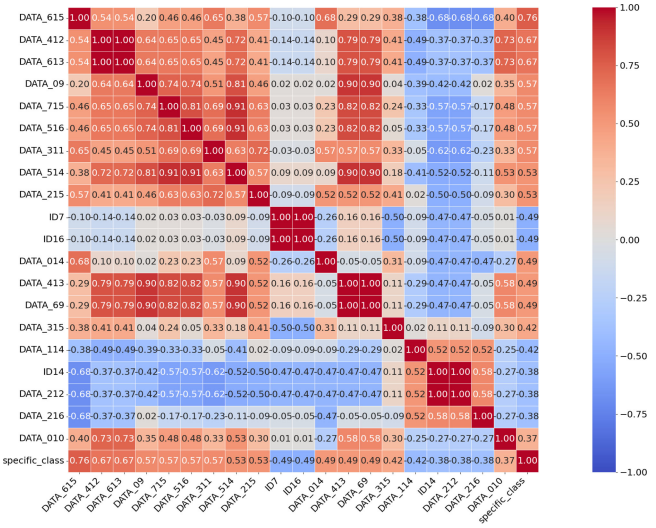


Fig. 6. PCC analysis for the top 20 features most highly correlated with the target class.

technique preserves dataset integrity by providing a plausible estimate for missing data without significantly altering the overall distribution. Mean imputation involves calculating the mean of available values for each feature and using the mean to replace any missing entries in that feature as in (1). Let X be a feature with observed values $X_1, X_2, \ldots, X_m$ with $m \leq n$

$$\bar{X} = \frac{1}{m} \sum_{i=1}^{m} X_i. \tag{1}$$

For each missing value in X, replace it with $\bar{X}$. Categorical variables were one-hot encoded, and finally, features were normalized to a standard range.

C. Correlation Analysis In-Vehicle Scenario

After preprocessing, the PCC was computed to eliminate redundant features as a result of their high correlation. The PCC quantifies the linear relationship of two features X and Y in

$$r(X, Y) = \frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2 \sum (Y_i - \bar{Y})^2}} \tag{2}$$

where X_i, Y_i are individual observations, and $\bar{X}, \bar{Y}$ are the means of features X and Y, respectively.

Fig. 6 shows the top 20 features most highly correlated with the target based on their PCC and their pairwise correlations. However, the persistence of high feature-to-feature correlations suggests that PCC alone may still be influenced by indirect relationships, necessitating a more robust approach.

Partial correlation controls feature Z in (3) for practical scenarios like in-vehicle communication with multiple variables

$$r(X, Y|Z) = \frac{r(X, Y) - r(X, Z)r(Y, Z)}{\sqrt{\left(1 - r^2(X, Z)\right)\left(1 - r^2(Y, Z)\right)}}. \tag{3}$$

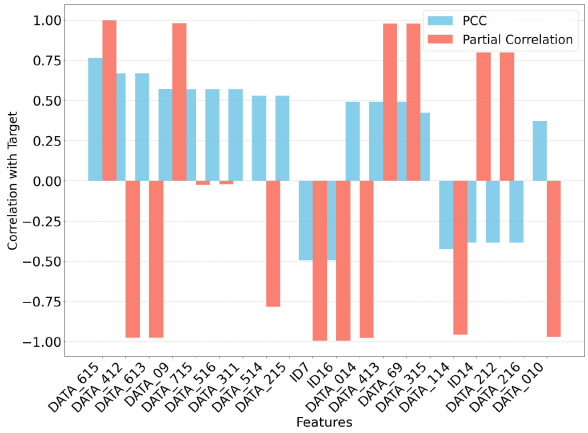


Fig. 7. PCC versus partial correlation for the top 20 features to assess feature relevance in the attack detection model.

For multiple control features $W_1, W_2, \ldots, W_n$, (4) gives the generalized partial correlation

$$r(X, Y|W) = \frac{r(X, Y) - r(X, W)r(Y, W)}{\sqrt{\left(1 - r^2(X, W)\right)\left(1 - r^2(Y, W)\right)}}. \tag{4}$$

Equation (5) determines the statistical significance of the feature correlation

$$t = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}} \tag{5}$$

where n is the sample size, and the degrees of freedom are given by $n - 2$.

While the PCC measures the overall linear relationship, partial correlation isolates the relationship by controlling for other variables, allowing for both bivariate and multivariate analysis. Fig. 7 illustrates the correlation analysis of the top 20 features selected based on their absolute PCC with the target, alongside their partial correlations, which control for the influence of other features.

Feature values between 0.75 and 1.00 exhibit strong positive correlations, indicating their initial relevance to the target. However, partial correlations for some features drop significantly below 0.50, highlighting the impact of multicollinearity and confounding variables in the multivariate dataset.

This discrepancy highlights the need for a hybrid approach, combining partial correlation with PCC as defined in (6). The hybrid approach scales PCC by the ratio of the absolute partial correlation to the absolute PCC, prioritizing features where the partial correlation preserves the original signal and penalizing those where it diminishes significantly. This refinement isolates direct relationships with the target attack classes and focuses on the most relevant features for enhancing the anomaly detection model's performance

$$\text{Hybrid PCC} = \text{PCC} \cdot \frac{|\text{Partial Corr}|}{|\text{PCC}|}. \tag{6}$$

If $|\text{PCC}| = 0$, the ratio is set to 0 to avoid division by zero.

D. Model Training

After the correlation analysis based on the combination of PCC and partial correlation, the prepruned decision tree

inspired by [14] was leveraged for model training. The choice of this model is based on its suitability for high-dimensional heterogeneous data in in-vehicle scenarios. Prepruning prevents overfitting in decision trees by limiting the tree's growth during the initial tree-building process. The maximum depth parameter (max-depth) controls how deep the tree can grow before stopping further node expansion [43].

$d(n) \leq d_{\max}$ constrains the tree depth, where $d(n)$ is node depth, and $d_{\max}$ is the max allowed depth. Node split criterion $f(S) = \arg\max [I(S_1) + I(S_2)]$ maximizes impurity reduction, where S_1, S_2 are subsets and $I()$ is the impurity measure. Equation (7) constrains the depth impurity reduction

$$\text{Split}(n) = \begin{cases} \max[I(S) - (I(S_1) + I(S_2))], & d(n) < d_{\max} \\ 0, & d(n) \geq d_{\max}. \end{cases} \quad (7)$$

Equation (8) gives the entropy-based information gain

$$H(S) = -\sum p_i \log_2 p_i, \quad IG = H(\text{parent}) - \sum \frac{|S_j|}{|S|} H(S_j) \quad (8)$$

where p_i is class proportion and expands the probability in

$$P_{\text{expand}} = \begin{cases} 1, & d(n) < d_{\max} \wedge I(S) > \theta \\ 0, & \text{otherwise.} \end{cases} \quad (9)$$

$N(d_{\max}) = 2^{(d_{\max}+1)} - 1$ preprunes the parent tree to max possible nodes for $d_{\max} = 20$, then $L(\text{tree}) = \text{Loss}(\text{tree}) + \alpha \cdot \text{depth(tree)}$ regularizes the tree depth and recursively splits in

$$S(n, d) = \begin{cases} \text{Split}(n), & d < d_{\max} \wedge |S| > \text{min\_samples} \\ \text{CreateLeafNode}(n), & \text{otherwise} \end{cases} \quad (10)$$

$\epsilon(\text{tree}) \leq C \cdot (\text{complexity(tree)}/n)$ generalizes possible errors and implements the entire process as decision_tree(X, y, max_depth=20) = Recursive_Split(X, y, depth=0, max_depth=20) considering the feature importance threshold, minimum samples per leaf and max_leaf nodes. Prepruning balances model complexity and generalization by limiting depth, refining splits, and applying regularization.

E. Blockchain Attack Logging and Malicious Node Isolation

1) Attack Logging: When a node is detected as malicious or behaving suspiciously, the IDS transmits an alert message to the blockchain network and logs a detection alert as in Algorithm 2. This ensures that every security incident is recorded on an immutable ledger, providing a reliable audit trail for further analysis and accountability.

2) Malicious Node Isolation: The malicious node is then isolated via the smart contract to prevent it from communicating with other network components. This isolation is recorded in a log with an active flag set to true, indicating that the isolation is currently in effect as in Algorithm 3. This is to stop the spread of malicious messages and safeguard the network's integrity by ensuring compromised nodes cannot interfere with other nodes.

Algorithm 2: Log Detection Alert

1: **procedure** LOGDETECTIONALERT(*ECU_address, message*)
2: RSU calls *logAlert(ECU_address, message)* **if** *ECU_address* ∈ *registeredECUs* **then**
3: *alertCounter* ← *alertCounter* + 1
4: *alerts*[*alertCounter*] ← *Alert(alertCounter, ECU_address, message, block.timestamp)*
5: Emit *AlertLogged(alertCounter, ECU_address, message)*
6: **end procedure**

Algorithm 3: Isolate Malicious Node

Require: ECU address, reason
Ensure: Node isolated
1: **procedure** ISOLATEMALICIOUSNODE
2: RSU calls ISOLATENODE(address, reason) **if** *ECU address* ∈ *registeredECUs* **then**
3: isolationCounter ← isolationCounter + 1
4: isolations[isolationCounter] ← ISOLATION(isolationCounter, ECU address, reason, block.timestamp, true)
5: Emit NODEISOLATED(isolationCounter, ECU address, reason)
6: **end procedure**

Algorithm 4: Lift Isolation of Node

Input: Isolation ID
Output: Isolation lifted
1 **Procedure Lift Isolation of Node:**
2 **begin**
3 RSU calls *liftIsolation(uint256)*
4 **if** *isolations[isolationId].active* **then**
5 *isolations[isolationId].active* ← false
6
7 **end**

3) Lifting Isolation: The isolation of a previously detected malicious node can be lifted once the ECU is detected as safe and not sending false data. The active flag of that isolation record is then set to false as in Algorithm 4. This change in status indicates that the ECU is no longer isolated and can resume normal communication within the network. This process ensures that once a node is deemed secure, it can be reintegrated, maintaining network efficiency without compromising security.

This approach enhances the integrity and traceability of security measures and leverages the blockchain's decentralized nature to prevent single points of failure and ensure robust protection against data falsification in the IVN. Additionally, by automating the isolation process through smart contracts, the system minimizes the response time to security incidents,

TABLE II
DISTRIBUTION OF ATTACKS IN THE EVALUATED DATASETS. ✓ INDICATES THE ATTACK IS PRESENT, WHILE ✗ INDICATES IT IS ABSENT

Attack Description	IoV			Non-IoV	
	CICIoV 2024	CAN-Intrusion	BurST ADMA	CICDDoS 2019	5G-NIDD
Denial of Service (DoS)	✓	✓	✗	✗	✓
Spoofing	✓	✓	✗	✗	✗
Fuzzy	✗	✓	✗	✗	✗
Position Falsification	✗	✗	✓	✗	✗
Distributed Denial of Service (DDoS)	✗	✗	✗	✓	✓
UDP Flood	✗	✗	✗	✗	✓
SYN Flood	✗	✗	✗	✗	✓
HTTP Flood	✗	✗	✗	✗	✓
UDP Scan	✗	✗	✗	✗	✓
TCP Connect Scan	✗	✗	✗	✗	✓
SYN Scan	✗	✗	✗	✗	✓
ICMP Flood	✗	✗	✗	✗	✓

thereby maintaining the overall safety and reliability of the IVN.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Data Description

The evaluation of the proposed scheme leveraged four other publicly available datasets in addition to the CICIoV2024 dataset to assess its performance across various scenarios. For IoV-specific datasets, CAN-intrusion, and BurST ADMA datasets were analyzed. The CAN-Intrusion dataset [25][3] was generated by capturing CAN traffic through the OBD-II port of an actual vehicle during the execution of message injection attacks. The BurST ADMA [44][4] dataset, a widely used resource for position falsification data, was employed to evaluate the model's ability to detect data falsification in intervehicular networks. To assess the robustness of the proposed approach in non-IoV contexts, the CICDDoS2019 and 5G-NIDD Datasets were incorporated into the study. The CICDDoS2019 [45][5] dataset contains DDoS attacks carried out using TCP/UDP-based protocols at the application layer. The 5G-NIDD dataset captures cyber attacks on a 5G testbed at the University of Oulu, Finland, with data collected from two base stations, each containing an attacker node and multiple benign users. Table II provides an overview of the evaluated datasets and the diverse attack types they encompass.

The preprocessed dataset was divided into training (70%) and testing (30%) sets.

B. Evaluation Metrics

An effective false data detection system should have high accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC) and Log-loss. MCC as shown in (11), provides a robust measure of the model's performance reliability. Unlike the F1-score, which can sometimes give inflated results on imbalanced datasets, the MCC offers a more balanced evaluation by effectively handling data imbalance

$$\text{MCC} = \frac{\text{TP.TN} - \text{FP.FN}}{\sqrt{(\text{TP}+\text{FP}).(\text{TP}+\text{FN}).(\text{TN}+\text{FP}).(\text{TN}+\text{FN})}}. \quad (11)$$

[3]https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset
[4]https://github.com/ahzam-a/BurST-ADMA
[5]https://www.unb.ca/cic/datasets/ddos-2019.html

TABLE III
PERFORMANCE OF THE DECISION TREE ALGORITHM WITHOUT FEATURE ENGINEERING

Datasets	Accuracy (%)	Log Loss	Time (s)
CICIoV2024	99.28	0.0431	3.77
CAN-Intrusion	98.63	0.054	4.99
BurST ADMA	98.41	0.0505	2.17
CICDDoS2019	98.68	0.0731	241.87
5G NIDD	95.61	0.431	14.436

Log-loss quantifies the accuracy of a model's predictions for DDoS attacks by penalizing the likelihood of incorrect classifications based on predicted probabilities as shown in

$$\text{Log-Loss} = -\frac{1}{N}\sum_{i=1}^{N}(y_i \log(p_i) + (1-y_i)\log(1-p_i)). \quad (12)$$

C. Proposed Model Performance Evaluation

The performance of the Decision tree across the investigated datasets without feature engineering is shown in Table III. Despite the notable accuracy and loss, computation time as a critical issue in vehicular communication scenarios remains a concern.

D. Impact of Feature Extraction

IoV connectivity introduces security vulnerabilities that can compromise vehicle and user privacy. As depicted in Fig. 1, these attacks are detected by analyzing communication data for deviations from normal behavior. Key features include traffic patterns (message frequency, packet size, flow), latency, protocol anomalies, signal strength, and vehicle behavior. Under normal conditions, these features are consistent, but attacks cause irregularities, like traffic spikes, altered flows, or unexpected packet sizes. The proposed approach leverages these features to recognize patterns and differentiate between normal communication and attacks, improving IoV security and reliability.

An in-depth analysis of the CICIoV2024 dataset was performed using the hybrid PCC approach to assess the relationship between minimal redundancy features and attack classes. The goal was to identify key features for attack detection via the proposed decision tree. Feature engineering techniques of Chi-squared (Chi), mutual information, ANOVA f-test, RFE, and principal component analysis (PCA) were employed to evaluate the prepruned decision trees across representative IoV datasets. Fig. 8 illustrates the relative importance of the top features for classifying and detecting in-vehicle attack instances. The optimal feature set (k-sample) balanced he performance and computation time.

Fig. 9 shows the computation time of the approach on the CICIoV2024 and CICDDoS2019 datasets. The result highlights the impact of FS on model performance, with the optimal computation time achieved using ten features and PCC having the shortest computation time among the techniques.

To assess the relationship between significant features and attack characteristics, we analyzed their distribution across different attack classes and normal communication

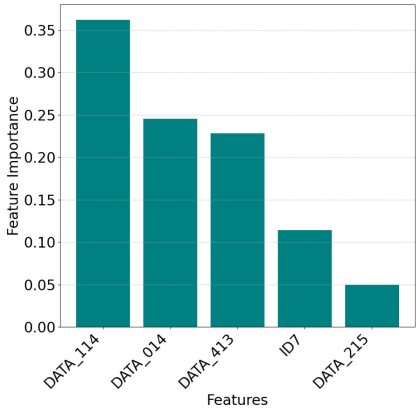


Fig. 8. Feature importance plot showing features with the most significant contributions for training the decision tree model.

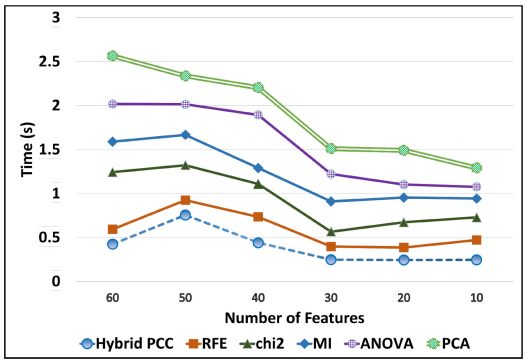


Fig. 9. Plot demonstrating the computation time performance of compared feature engineering techniques with k-samples of 60 to 10 features.

(Benign). Fig. 10(f) highlights the distinct patterns, demonstrating the features' effectiveness in attack detection within the CICIoV2024 dataset.

Benign samples consistently cluster around 0.0 across all features, reflecting typical in-vehicle communication behavior under normal conditions. In contrast, attack classes exhibit prominent peaks at 1.0 for specific features: DATA_114 and DATA_413 show a dominant peak for *Spoofing_RPM*, DATA_014 and DATA_215 peak for *Spoofing_STEERING_WHEEL*, and ID7 highlights *Spoofing_SPEED*. These peaks at 1.0 suggest that the features capture extreme or falsified values characteristic of spoofing attacks, where malicious data manipulates critical CAN bus parameters such as RPM, steering angle, or speed. The bimodal nature of some distributions reflecting peaks at both 0.0 and 1.0 indicates the Decision Tree model's ability to leverage these differences to distinguish between normal and attack instances in the dataset.

Employing the PCC feature engineering to representative machine learning models on the CICIoV2024 dataset significantly reduced the computation time and improved the detection accuracy as in Table IV. It highlights the relevance of the proposed PCC feature engineering for swift detection of data falsification with ≤ 1 s computation time in most of the models and ≤ 0.1 s when combined with the Decision tree.

Table V presents the performance results across the evaluated datasets, with and without FS. The performance is

TABLE IV
PERFORMANCE ANALYSIS OF THE PCC FEATURE ENGINEERING WITH VARIOUS ALGORITHMS ON THE CICIOV2024 DATASET

Model	Accuracy (%)	MCC (%)	Time(s)
DT	**99.99**	**99.99**	**0.0015**
RF	99.99	99.99	0.390
LR	99.99	99.99	0.390
NB	95.40	93.44	0.9680
KNN	99.99	99.99	0.6942
XGBOOST	99.99	99.99	8.169

TABLE V
FEATURE ENGINEERING PERFORMANCE IMPACT ON BOTH IOV AND NON-IOV DATA FALSIFICATION DATASETS

Datasets	Metrics	Performance	
		Without FS	**With FS**
CICIoV2024	Accuracy	99.28	**99.99**
	F1-Score	99.28	**99.99**
	MCC	97.55	**99.99**
	Time (s)	3.77	**0.245**
	Loss	0.0431	**0.0015**
CAN-Intrusion	Accuracy	96.60	**99.96**
	F1-Score	96.60	**99.96**
	MCC	93.44	**99.89**
	Time (s)	4.99	**1.3228**
	Loss	0.0635	**0.0104**
BurST ADMA	Accuracy	98.41	**99.31**
	F1-Score	95.37	**99.31**
	MCC	76.98	**96.81**
	Time (s)	2.17	**0.859**
	Loss	0.1506	**0.0507**
CICDDoS2019	Accuracy	98.68	**99.14**
	F1-Score	98.68	**99.14**
	MCC	98.24	**98.86**
	Time (s)	1.766	**0.3178**
	Loss	0.1041	**0.0731**
5G-NIDD	Accuracy	95.61	**99.95**
	F1-Score	95.61	**99.95**
	MCC	93.79	**98.86**
	Time (s)	14.436	**2.637**
	Loss	0.431	**0.0144**

TABLE VI
PERFORMANCE COMPARISON WITH SURVEYED STUDIES

Technique	Dataset	Accuracy (%)	F1-score (%)	Time(s)
RFE+DT [28]	CICIDS2017	99.58	99.6	1011.1
RFE+DT [28]	CAN-Intrusion	99.86	99.9	105.7
FS Stacking [29]	CICIDS2017	99.98	99.7	2774.8
PCC+RF [5]	VeReMi	91.06	85.95	x
PCC+Ens.RF [27]	VeReMi	99.62	x	6.9
Hybrid PCC+DT	**CICIoV2024**	**99.99**	**99.99**	**0.245**
Hybrid PCC+DT	**CAN-Intrusion**	**99.96**	**99.96**	**1.322**
Hybrid PCC+DT	**BurST ADMA**	**99.31**	**99.31**	**0.859**
Hybrid PCC+DT	**CICDDoS2019**	**99.14**	**99.14**	**0.3178**
Hybrid PCC+DT	**5G-NIDD**	**99.95**	**99.95**	**2.637**

measured across accuracy, F1-score, MCC, time, and loss metrics. The proposed PCC feature engineering consistently improved all metrics across all datasets, highlighting the effectiveness of selecting relevant features for data falsification detection. The demonstrated effectiveness of PCC feature engineering in detecting data falsification within IoV and non-IoV scenarios significantly enhances the overall performance and trustworthiness of 6G-enabled applications.

A comparative analysis in Table VI highlights the effectiveness of the proposed hybrid PCC combined with a prepruned decision tree for detecting data falsification in IVNs. This approach outperforms existing FS techniques, achieving near-perfect accuracy of 99.99% and an F1-score of 99.96%,

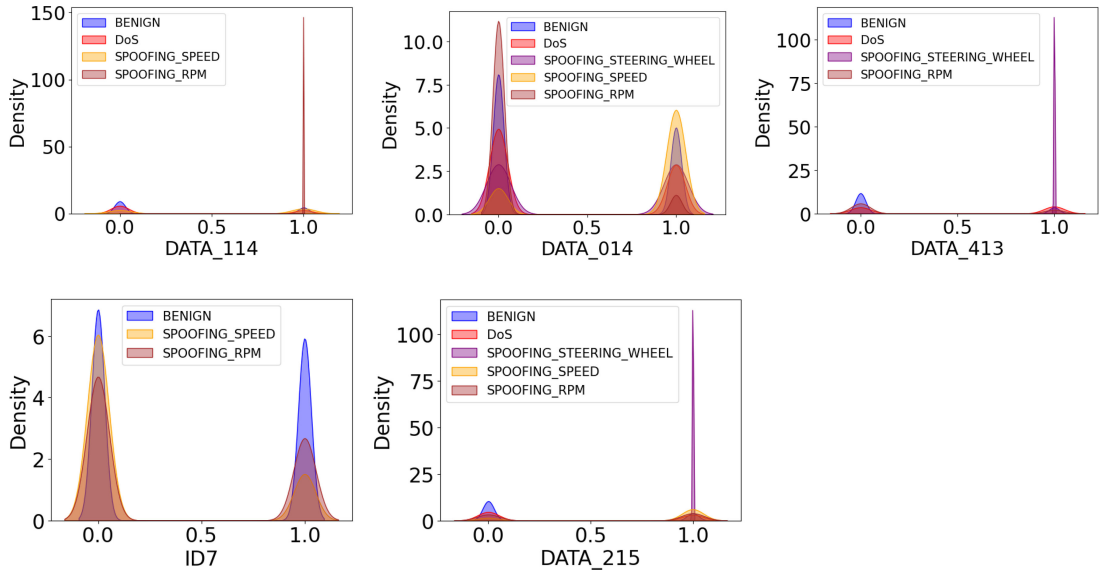


Fig. 10. Distribution of the most significant features across existing attack classes in the CICIoV2024 dataset.

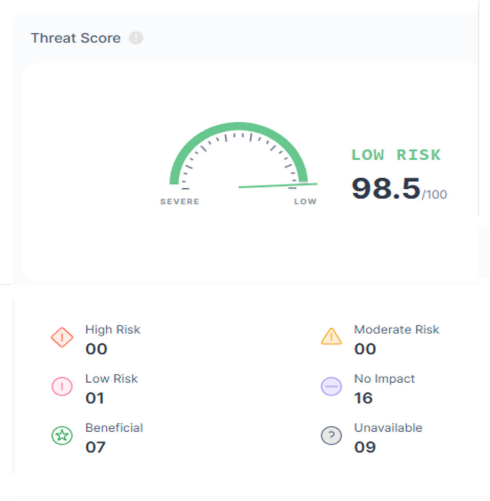


Fig. 11. Threat analysis result of the smart contract.

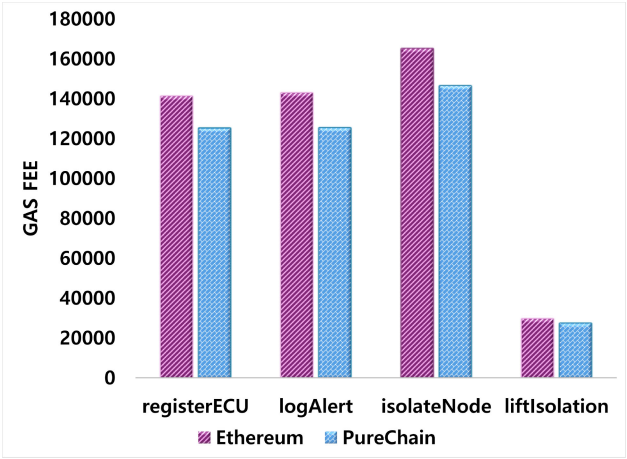


Fig. 12. Gas cost for purechain versus ethereum.

surpassing RFE+DT and FS Stacking. It demonstrates robustness across multiple datasets with accuracies of 99.31% and F1-scores of 99.14%. Additionally, it shows competitive

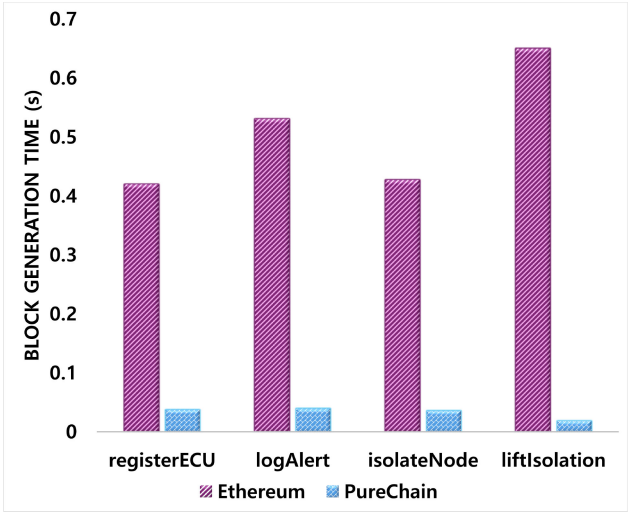
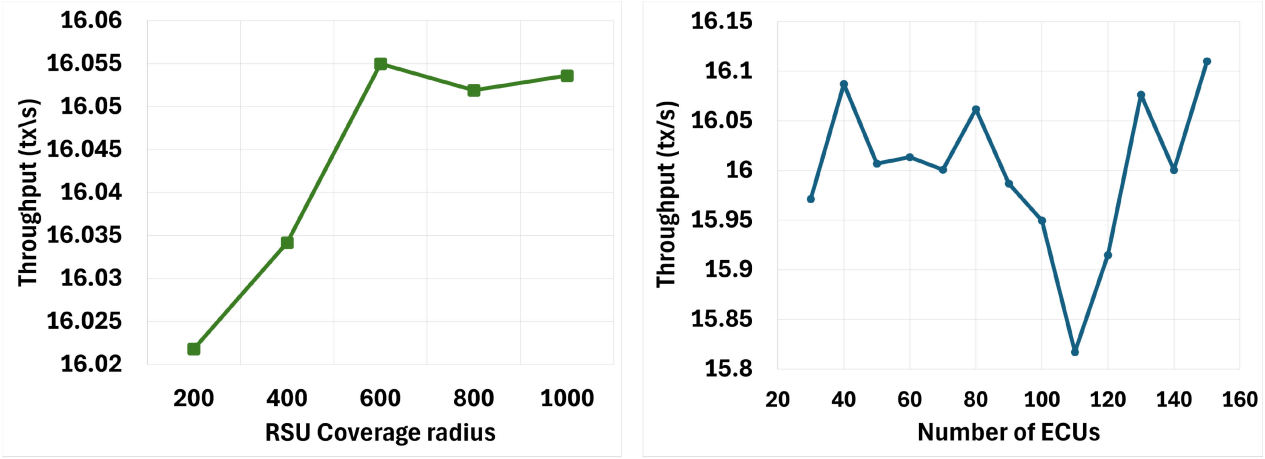


Fig. 13. Block generation time for purechain versus ethereum.

processing times of 0.245 s for CICIoV2024 and 1.322 s for CAN-Intrusion, ensuring efficiency. The results confirm the method's suitability for enhancing security and reliability in 6G IVNs, making it well-suited for connected and autonomous vehicles.

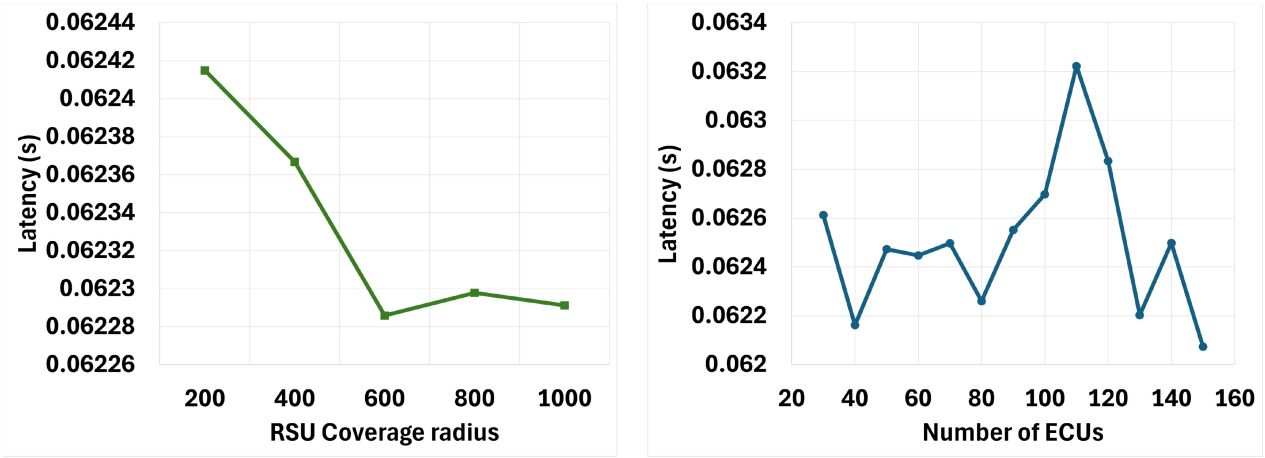
E. Blockchain Evaluation

The performance of the blockchain component within our proposed framework was rigorously evaluated by analyzing gas fees and block generation times across key smart contract functions, such as *registerECU*, *logAlert*, *isolateNode*, and *liftIsolation*. Identical smart contracts were deployed on two blockchain platforms: 1) PureChain, a private permissioned blockchain tailored for efficiency [46], which is proposed in this study and 2) ethereum, a widely adopted public network. Public blockchains suffer from scalability constraints and significant delays which can be mitigated using PureChain. The evaluation was conducted on a system equipped with an



(a) (b)

Fig. 14. Impact of RSU coverage, and increasing ECU density on PureChain transaction throughput. (a) RSU coverage. (b) Increasing ESU density.



(a) (b)

Fig. 15. Impact of RSU coverage and increasing ECU density on PureChain transaction latency. (a) RSU coverage. (b) Increasing ESU density.

Intel Core i5-8500 CPU @ 3.00 GHz and 32 GB RAM and NVIDIA GeForce GTX 1050, operating on Windows 11 Pro. Ganache acted as a local Ethereum environment to simulate effectively simulate Ethereum transactions. The smart contract was deployed using Remix IDE.

A threat analysis was performed to assess the vulnerability of the smart contract to potential exploitation. As shown in Fig. 11, the scan yielded a *LowRisk* threat score of 98.5 out of 100, indicating a highly secure implementation with minimal vulnerabilities.

Gas fees, representing the computational cost of executing smart contracts and transactions on the blockchain, are a critical metric for assessing the economic feasibility and scalability of the system in a resource-constrained vehicular environment. Fig. 12 presents a comparative analysis of gas fees between Ethereum and PureChain. Ethereum consistently incurs higher gas costs, particularly for *isolateNode*, which demands significant computational resources to isolate malicious ECUs in real-time. In contrast, PureChain demonstrates superior gas efficiency across all functions, with *registerECU* and *logAlert* exhibiting only marginal differences and *liftIsolation* registering the lowest fees on both platforms. These results underscore PureChain's optimization of contract execution, substantially reducing transaction costs relative to Ethereum, an essential advantage for the high-frequency, low-latency demands of 6G IoV networks where cost efficiency directly impacts scalability and deployment viability.

To further evaluate blockchain performance, the block generation time, the average duration required to create and add a new block to the chain, was assessed for each smart contract function. This metric is pivotal, as lower block generation times expedite transaction confirmation, enhance network security, and bolster system efficiency, which is paramount for real-time intrusion mitigation in safety-critical vehicular applications.

As illustrated in Fig. 13, Ethereum exhibits markedly higher block generation times, ranging from 0.4 to 0.65 s, attributable to its computationally intensive proof-of-work consensus mechanism. Conversely, PureChain achieves significantly lower latency, processing transactions faster due to its

TABLE VII
RSU COVERAGE AND ECU SIMULATION: IMPACT OF VARYING RSU COVERAGE (200, 400, 600, 800, AND 1000 M) ON AREA COVERAGE, VEHICLE COUNT, AND TOTAL ECUS (50 ECUS PER VEHICLE)

RSU Coverage	Area Covered (km^2)	Vehicles	Total ECUs (= Vehicles × 50 ECUs)
200 m	0.125 km^2	~62 vehicles	~3100 ECUs
400 m	0.502 km^2	~251 vehicles	~12550 ECUs
600 m	1.131 km^2	~565 vehicles	~28250 ECUs
800 m	2.010 km^2	~1005 vehicles	~50250 ECUs
1000 m	3.141 km^2	~1570 vehicles	~78,500 ECUs

PoA^2 consensus mechanism. The PoA^2 mechanism enhances PureChain's suitability for 6G IoV by integrating a standby validator that monitors network participants and an idle redundant signer to replace inactive validators, ensuring uninterrupted operation and resilience against mining disruptions.

The scalability of the blockchain-enhanced IDS framework was evaluated by analyzing its ability to handle increasing ECUs per RSU and the impact of RSU coverage (200, 400, 600, 800, and 1000 m) on blockchain performance under realistic vehicular densities. The simulation assumed that each ECU sends one transaction, with an average of 50 ECUs per car actively performing transactions. Simulations assuming 500 vehicles per km^2 in urban areas and RSU coverage between 200 and 1000 m, are presented in Table VII. Throughput, defined as the average number of transactions per second (tx/s), and transaction latency, the time taken for each blockchain transaction, were evaluated as the number of ECUs per RSU increased.

Fig. 14 shows that throughput remains relatively stable, fluctuating between 15.9 and 16.15 tx/s as ECU density increases, without noticeable degradation. As RSU coverage expands beyond 600 m, throughput stabilizes above 16.05 tx/s, indicating the possibility of larger coverage areas facilitating more efficient ECU transaction aggregation and reducing consensus overhead. Therefore, the system maintains a high transaction processing capability under both increasing ECU load and expanded RSU coverage, demonstrating strong scalability with minimal performance loss.

As shown in Fig. 15, transaction latency remains consistently low, ranging from approximately 0.0618 to 0.063 s as ECU density increases. These minor fluctuations indicate the system's ability to maintain real-time responsiveness even under higher transaction loads. With expanding RSU coverage, latency slightly decreases and stabilizes beyond 600 m, suggesting improved consensus efficiency due to broader communication reach. Overall, the system demonstrates low and predictable latency across both ECU and RSU scaling scenarios, confirming its suitability for 6G IVNs.

This design improves scalability and efficiency, while also fortifying security and reliability. These are crucial for managing ECU registration, logging intrusion alerts, and isolating malicious nodes in response to CAN Bus threats. The evaluation results affirm that PureChain's lower gas fees, faster block generation times and high scalability enable our system to meet the stringent real-time requirements of 6G IoV, outperforming Ethereum in cost-effectiveness and operational agility. These results validate the proposed framework's efficacy in securing IVNs, demonstrating its potential to advance the safety and dependability of intelligent transportation systems within the 6G paradigm.

V. CONCLUSION

This study advances the detection and mitigation of data falsification in 6G IVNs by integrating a feature-engineered IDS with blockchain technology, with a focus on minimizing computational overhead. The proposed IDS, deployed on the TCU as a gateway ECU, leverages 6G's URLLC to enable real-time threat detection through an optimized PCC and a prepruned decision tree algorithm, achieving a balance between accuracy and efficiency. Security was enhanced through PureChain, a private blockchain network that utilizes the PoA^2 consensus mechanism, deployed on RSUs to log ECU data and securely isolate malicious ECUs. This approach outperformed Ethereum in terms of gas fees and block generation times and showed high scalability with increasing ECU transactions. The framework demonstrates efficacy in enhancing IVN security while optimizing resources, offering a scalable solution for 6G IoV networks. Future work will explore adaptive machine learning algorithms to address emerging threats, ensuring resilience in dynamic 6G IoV environments, thus laying the foundation for securing next-generation IVNs.

REFERENCES

[1] S. M. Mohammed, A. Al-Barrak, and N. T. Mahmood, "Enabling technologies for ultra-low latency and high-reliability communication in 6G networks," *Ingenierie des Systemes d'Information*, vol. 29, pp. 1195–1208, Jun. 2024.

[2] Z. Sun et al., "A data attack detection framework for cryptography-based secure aggregation methods in 6G intelligent applications," *Electronics*, vol. 13, no. 11, p. 1999, 2024.

[3] Q. Dong, Z. Song, and H. Shao, "Intrusion detection and defence for CAN bus through frequency anomaly analysis and arbitration mechanism," *Electron. Lett.*, vol. 60, no. 3, 2024, Art. no. e13112.

[4] *SAE International Technical Standard: Communications Message Set Dictionary*, SAE Standard j2735_202309 V2X, 2023.

[5] E. Abdelkreem, S. Hussein, and A. Tammam, "Feature engineering impact on position falsification attacks detection in vehicular ad-hoc network," *Int. J. Inf. Secur.*, vol. 23, pp. 1939–1961, Mar. 2024.

[6] Y. Lee and S. Woo, "CAN signal extinction-based DoS attack on in-vehicle network," *Secur. Commun. Netw.*, vol. 2022, Sep. 2022, Art. no. 9569703, doi: 10.1155/2022/9569703.

[7] B. Ji et al., "Survey on the Internet of Vehicles: Network architectures and applications," *IEEE Commun. Stand. Mag.*, vol. 4, no. 1, pp. 34–41, Mar. 2020.

[8] A. K. Dwivedi, "Anomaly detection in intra-vehicle networks," 2022, *arXiv:2205.03537*.

[9] J. Sun, S. Iqbal, N. S. Arabi, and M. Zulkernine, "A classification of attacks to in-vehicle components (IVCs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100253.

[10] S. Mumtaz, M. I. Ashraf, V. G. Menon, T. Abbas, and A. Al-Dulaimi, "Guest editorial introduction to the special issue on intelligent autonomous transportation system with 6G," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1585–1586, Feb. 2022.

[11] M. Chowdhury, A. Apon, and K. Dey, "Security and privacy solutions," in *Data Analytics for Intelligent Transportation Systems*. Amsterdam, The Netherlands: Elsevier, 2017.

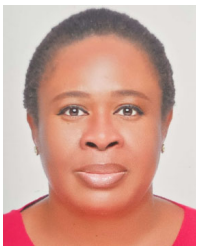
[12] G. Dhivyasri, R. Mariappan, and R. Sathya, "Telematic unit for advanced fuel level monitoring system," in *Proc. IEEE 9th Int. Conf. Intell. Syst. Control (ISCO)*, 2015, pp. 1–7.

[13] Y. G. Damtew, H. Chen, and Z. Yuan, "Heterogeneous ensemble feature selection for network intrusion detection system," *Int. J. Comput. Intell. Syst.*, vol. 16, p. 9, Feb. 2023.

[14] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Agnostic CH-DT technique for SCADA network high-dimensional data-aware intrusion detection system," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10344–10356, Jun. 2023.
[15] Y. Liu, S. Peng, M. Zhang, S. Shi, and J. Fu, "Towards secure and efficient integration of blockchain and 6G networks," *PLoS One*, vol. 19, Apr. 2024, Art. no. e0302052.
[16] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of blockchain in IoT cybersecurity," *Sensors*, vol. 24, p. 3111, May 2024.
[17] K. Shah, S. Chadotra, S. Tanwar, R. Gupta, and N. Kumar, "Blockchain for IoV in 6G environment: Review solutions and challenges," *Clust. Comput.*, vol. 25, no. 3, pp. 1927–1955, 2022.
[18] A. Sangwan, A. Sangwan, and R. P. Singh, "A classification of Misbehavior detection schemes for VANETs: A survey," *Wireless Pers. Commun.*, vol. 129, no. 1, pp. 285–322, 2023.
[19] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernández-Ramos, and V. Kouliaridis, "Demystifying in-vehicle intrusion detection systems: A survey of surveys and a meta-taxonomy," *Electronics*, vol. 11, no. 7, p. 1072, 2022.
[20] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Comput. Surveys*, vol. 55, no. 11, pp. 1–40, 2023.
[21] F. Luo, J. Wang, X. Zhang, Y. Jiang, Z. Li, and C. Luo, "In-vehicle network intrusion detection systems: A systematic survey of deep learning-based approaches," *PeerJ Comput. Sci.*, vol. 9, Oct. 2023, Art. no. e1648.
[22] S. Anbalagan, G. Raja, S. Gurumoorthy, R. D. Suresh, and K. Dev, "IIDS: Intelligent intrusion detection system for sustainable development in autonomous vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 15866–15875, Dec. 2023.
[23] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Real-time position falsification attack detection system for Internet of Vehicles," in *Proc. 26th IEEE Int. Conf. Emerg. Technol. Fact. Autom. (ETFA)*, 2021, pp. 1–4.
[24] H. L. Nakayiza, L. Ahakonye, D.-S. Kim, and J. M. Lee, "Machine learning algorithms for detecting intra-vehicular data falsification," in *Proc. Korean Inst. Commun. Inf. Sci. Summer Conf. (KICS)*, 2024, pp. 1088–1089.
[25] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198.
[26] P. Dhal and C. Azad, "A comprehensive survey on feature selection in the various fields of machine learning," *Appl. Intell.*, vol. 52, no. 4, pp. 4543–4581, 2022.
[27] G. Anyanwu, C. 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 Exp.*, vol. 9, pp. 122–129, Feb. 2023.
[28] J. Liu and W. Fan, "A machine learning-based intrusion detection approach for intelligent connected vehicles," in *Proc. 24st Asia-Pac. Netw. Oper. Manage. Symp. (APNOMS)*, 2023, pp. 231–234.
[29] L. Yang, A. Moubayed, I. Hamieh, and A. Shami, "Tree-based intelligent intrusion detection system in Internet of Vehicles," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.
[30] H. L. Nakayiza, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Blockchain-enabled intrusion detection system for distributed vehicular networks," in *Proc. Korean Inst. Commun. Sci. Conf.*, 2024, pp. 463–464.
[31] 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.
[32] M. Salem, M. Mohammed, and A. Rodan, "Security approach for in-vehicle networking using blockchain technology," in *Proc. 7th Int. Conf. Emerg. Internet, Data Web Technol. (EIDWT)*, 2019, pp. 504–515.
[33] T. Su, S. Shao, S. Guo, and M. Lei, "Blockchain-based Internet of Vehicles privacy protection system," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–10, Sep. 2020, doi: 10.1155/2020/8870438.
[34] S. Anbalagan, G. Raja, S. Gurumoorthy, R. D. Suresh, and K. Ayyakannu, "Blockchain assisted hybrid intrusion detection system in autonomous vehicles for industry 5.0," *IEEE Trans. Consum. Electron.*, vol. 69, no. 4, pp. 881–889, Nov. 2023.
[35] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, "Blockchain integration for in-vehicle CAN bus intrusion detection systems with ISO/SAE 21434 compliant reporting," *Sci. Rep.*, vol. 14, p. 8169, Apr. 2024.
[36] N. Xie, C. Zhang, Q. Yuan, J. Kong, and X. Di, "IoV-BCFL: An intrusion detection method for IoV based on blockchain and federated learning," *Ad Hoc Netw.*, vol. 163, Oct. 2024, Art. no. 103590.
[37] B. Lampe and W. Meng, "Intrusion detection in the automotive domain: A comprehensive review," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 4, pp. 2356–2426, 4th Quart., 2023.
[38] Q. Yang, S. Fu, H. Wang, and H. Fang, "Machine-learning-enabled cooperative perception for connected autonomous vehicles: Challenges and opportunities," *IEEE Netw.*, vol. 35, no. 3, pp. 96–101, May/Jun. 2021.
[39] 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 *Proc. 43rd IEEE Int. Conf. Consum. Electron. (ICCE)*, 2025, pp. 1–6.
[40] D.-S. Kim and R. Syamsul, "Integrating machine learning with proof-of-authority-and-association for dynamic signer selection in blockchain networks," *ICT Exp.*, vol. 11, pp. 258–263, Apr. 2025.
[41] M. A. P. Putra, R. N. Alief, S. M. Rachmawati, G. A. Sampedro, D.-S. Kim, and J.-M. Lee, "Proof-of-authority-based secure and efficient aggregation with differential privacy for federated learning in industrial IoT," *Internet Things*, vol. 25, Apr. 2024, Art. no. 101107.
[42] E. C. P. Neto et al., "CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV can bus," *Internet Things*, vol. 26, Jul. 2024, Art. no. 101209.
[43] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "SCADA intrusion detection scheme exploiting the fusion of modified decision tree and chi-square feature selection," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100676.
[44] M. A. Amanullah, M. B. Chhetri, S. W. Loke, and R. Doss, "BurST-ADMA: Towards an Australian dataset for misbehaviour detection in the Internet of Vehicles," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops Affil. Events (PerCom Workshops)*, 2022, pp. 624–629.
[45] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *Proc. Int. Carnahan Conf. Security Technol. (ICCST)*, 2019, pp. 1–8.
[46] S. I. Igboanusi, G. O. Anyanwu, D. T. Etobi, and D.-S. Kim, *Pure Chain Ecosystem*, Kumoh Nat. Inst. Technol., Gumi, South Korea, 2023.

Hope Leticia Nakayiza received the Bachelor of Software Engineering (B.Eng.) degree from Kangnam University, Yongin, South Korea, in 2023. She is currently pursuing the master's degree in IT-convergence engineering with the Networked System Laboratory of the IT-Convergence Engineering Department, Kumoh National Institute of Technology, Gumi, South Korea.

Her current research interests are artificial intelligence and blockchain application and optimization for the Internet of vehicles security.



Love Allen Chijioke Ahakonye (Member, IEEE) received the B.Sc. degree in mathematics/computer science from the University of Port Harcourt, Port Harcourt, Nigeria, in 2001, the M.Sc. degree in information technology from the Federal University of Technology, Gaga, Nigeria, in 2016, and the Ph.D. degree in IT-convergence engineering from the Networked System Laboratory, IT-Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea, in 2024.

She has over a decade of experience in the Nigerian oil and gas sector as a Network and System Administrator from 2002 to 2016. In 2017, she briefly was a Logistics Superintendent with the Nigerian Petroleum Development Company, Benin City, Nigeria, until 2019. She is also a Postdoctoral Researcher with the ICT Convergence Research Center, Kumoh National Institute of Technology. Her research interest is artificial intelligence application to the Internet of Things (IoT) and industrial IoT, supervisory control and data acquisition, and industrial control system for intrusion/anomaly detection, cyber-security, fault detection, XAI, and manufacturing execution systems.

Dr. Ahakonye is a member of the Computer Professionals Registration Council of Nigeria.

Dong-Seong Kim (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2003.

From 1994 to 2003, he was a Full-Time Researcher with the ERC-ACI, Seoul National University. From March 2003 to February 2005, he served as a Postdoctoral Researcher with the Wireless Network Laboratory in the School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA. From 2007 to 2009, he was a Visiting Professor with the Department of Computer Science, University of California at Davis, Davis, CA, USA. He served as the Dean of IACF, Nottinghamshire, U.K.,from 2019 to 2022. He is currently a Professor with the Department of IT Convergence Engineering, the School of Electronic Engineering, Kumoh National Institute of Technology, Gumi, South Korea, where he is also the Director of the KIT Convergence Research Institute and the ICT Convergence Research Center (ITRC and NRF Advanced Research Center Program), supported by the Korean Government, and the Director of NSLab Company Ltd., Gumi. His primary research interests include real-time IoT and smart platforms, industrial wireless control networks, networked embedded systems, fieldbus, metaverse, and blockchain.

Prof. Kim is a Senior Member of ACM.

Jae-Min Lee (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2005.

From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea, where he was a Principal Engineer from 2015 to 2016. Since 2017, he has been an Associate Professor with the School of Electronic Engineering and the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, Gyeongbuk, South Korea. Since 2024, he has been the Director of the Smart Defense Logistics Innovation Convergence Research Center (ITRC Program). He is the Executive Director of the Korean Institute of Communications and Information Sciences. His current main research interests are smart IoT convergence application, industrial wireless control network, UAV, metaverse, and blockchain.