Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 11, No. 04, December 2025.

FEDERATED-LEARNING MODELS FOR DISTRIBUTED VANET SECURITY

Moawiah El-Dalahmeh and Adi El-Dalahmeh

(Received: 15-Jul.-2025, Revised: 8-Nov.-2025, Accepted: 9-Nov.-2025)

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) are a cornerstone of modern Intelligent Transportation Systems (ITSs), enabling real-time communication among vehicles and infrastructure. However, the open and dynamic nature of VANETs exposes them to a wide range of cybersecurity threats, such as spoofing, Sybil attacks and denial-of-service (DoS). This paper introduces a novel Federated Learning (FL) framework designed to enhance VANET security by enabling distributed and privacy-preserving intrusion detection across the network. By leveraging local model updates instead of centralized data aggregation, our proposed FL approach mitigates privacy risks, reduces communication overhead and offers robust detection of cyber-threats. The paper presents a comprehensive analysis including system architecture, threat modeling, security properties, performance evaluation and real-world applicability. Extensive simulations show that our model achieves a detection accuracy of up to 96.2%*, with minimal latency and low model convergence time, outperforming existing centralized and traditional machine-learning models.*

KEYWORDS

Federated learning, VANET, Intrusion-detection system, Cybersecurity, Distributed AI, Privacy preservation, Edge computing.

1. INTRODUCTION

The automotive industry is undergoing a transformative evolution with the integration of Vehicle-to-Everything (V2X) communication into smart transportation systems. Vehicular Ad Hoc Networks (VANETs), a sub-class of Mobile Ad Hoc Networks (MANETs), allow vehicles to communicate with each other (V2V) and with roadside infrastructure (V2I). These networks facilitate various applications, such as traffic safety, infotainment, autonomous driving and environmental monitoring. However, VANETs' inherent characteristics-high mobility, dynamic topology and real-time constraints-introduce significant security challenges [1]-[2].

Traditional centralized Intrusion-detection Systems (IDS) struggle to meet the privacy and scalability demands of VANETs [3]. Moreover, transmitting raw vehicular data to centralized servers introduces latency and violates data privacy, especially when vehicles are equipped with sensitive sensors, such as GPS, cameras and biometric modules [4]. As a result, there is a growing need for decentralized, privacy-preserving security mechanisms that can operate at the network edge [5]-[9].

Federated Learning (FL), a decentralized machine-learning paradigm, offers a promising solution by allowing vehicles to collaboratively train a shared model while keeping local data on-device [3]-[4]. Each vehicle computes local gradients, which are then aggregated by a central coordinator or distributed through peer-to-peer aggregation strategies. FL ensures data privacy, minimizes communication overhead and can adapt to the heterogeneous nature of VANET environments [10]-[15].

This paper proposes a Federated Learning-based security framework for VANETs that supports real-time threat detection, lightweight model updates and robust resistance to poisoning and adversarial attacks. Our key contributions include:

- A novel federated intrusion-detection architecture tailored for distributed VANET environments.
- Integration of lightweight deep-learning models with differential privacy and secure aggregation techniques.
- Comprehensive mathematical modeling and performance analysis under various attack scenarios.

M. El-Dalahmeh and A. El-Dalahmeh are with Department of Cybersecurity, Al-Zaytoonah University of Jordan, Amman, Jordan. Email: M.eldalahmeh@zuj.edu.jo and A.eldalahmeh@zuj.edu.jo

- Evaluation using real-world VANET datasets (e.g. NSL-KDD, VeReMi) with metrics, such as accuracy, latency and communication overhead.
- Comparison with centralized and traditional IDS approaches demonstrating the superiority of FL in distributed environments.

The remainder of this paper is organized as follows. Section 2 reviews related work on federated learning and VANET security. Section 3 describes the system model and methodology. Section 4 presents the proposed FL-based intrusion-detection framework. Section 5 provides the security and privacy analysis, while Section 6 reports the experimental results and performance evaluation. Section 7 discusses reproduction with real-world VANET data. Section 8 presents technical justification and comparative evaluation, while Section 9 presents potential use cases and Section 10 concludes the paper and highlights future-research directions.

2. RELATED WORKS

2.1 VANET Security Challenges

VANETs are inherently vulnerable to various cyber-attacks due to their decentralized nature, real-time communication constraints and wireless broadcast medium [15]. Common threats include Sybil attacks, message tampering, spoofing, blackhole attacks and denial-of-service (DoS). Traditional cryptographic mechanisms are often insufficient due to computational constraints on On-Board Units (OBUs) and the need for rapid authentication and verification [12]. Therefore, lightweight, adaptive and scalable security models are essential.

2.2 Intrusion-detection Systems (IDSs) in VANETs

Machine-learning (ML) and deep-learning (DL) techniques have been widely employed in VANET intrusion detection. Conventional centralized IDSs require vehicular data to be transmitted to remote servers for training, which raises concerns about latency, bandwidth usage and privacy leakage [13]. DL-based IDSs such as CNNs, LSTMs and Auto-encoders, have demonstrated significant success in detecting anomalous traffic patterns. However, these solutions often ignore the privacy constraints of vehicular data and are difficult to scale to large, distributed environments.

2.3 Federated Learning in Intelligent Networks

Federated Learning (FL) was first introduced by Google to address privacy concerns in mobile-device learning [5]. Since then, FL has gained attention in smart healthcare, finance and IoT systems. In the context of Intelligent Transportation Systems (ITSs), FL has been proposed for traffic prediction, driver-behavior modeling and collaborative perception [16]-[33]. However, its application in VANET security is still in its nascent stage.

Several studies have explored FL in vehicular environments. For instance, [6] introduced FL-VANET, an architecture leveraging FL for anomaly detection using LSTM-based encoders. [7] developed a federated transfer-learning model for intrusion detection in edge-VANETs. Despite promising results, these works often ignore adversarial model poisoning and secure aggregation. Moreover, the dynamic and heterogeneous nature of VANET nodes requires models that can handle non-IID data and intermittent participation [34]-[42].

2.4 Secure Federated Learning in VANETs

Privacy and security in FL are emerging concerns. Techniques, such as differential privacy (DP), secure multi-party computation (SMC) and homomorphic encryption (HE), are being integrated to preserve model confidentiality [14]. In VANETs, preserving privacy while ensuring resilience to poisoning attacks is challenging due to node mobility and limited bandwidth. Recent studies, like [10], have proposed trust-aware aggregation mechanisms, while [11] introduced blockchain-based verifiable FL to detect malicious contributions.

Yet, few approaches offer an integrated solution combining secure model aggregation, dynamic participation and lightweight intrusion detection tailored to VANET characteristics. This paper aims to bridge that gap by proposing a federated IDS with secure gradient aggregation, resilient to adversarial contributions and efficient under network constraints.

2.5 Comparison Summary

Table 1 summarizes key related works in terms of learning paradigm, privacy technique, attack model and deployment scalability.

Table 1. Comparison of related works in FL-based VANET security.

Approach	Learning Model	Privacy Mechanism	Limitations
Wang et al. (2024) [6]	LSTM + FL	None	Lacks defense against poisoning attacks
Zhou et al. (2023) [7]	Transfer + FL	Differential Privacy (DP)	High communication overhead
Rahman et al. (2023) [10]	CNN + FL	Trust Aggregation	No protection against Sybil attacks
Ahmed et al. (2023) [11]	FL + Blockchain	Verifiable Updates	High computational complexity
This Work	CNN + FL	DP + Secure Aggregation	VANET optimized integrated framework

3. METHODOLOGY

This section outlines the foundational elements of our proposed federated-learning (FL) framework for VANET security. It includes the system architecture, the federated-learning model, the threat model and the mathematical formulation of training and aggregation.

3.1 System Model

Our system consists of three main components:

- Vehicles (Clients): Each vehicle is equipped with an On-Board Unit (OBU) and local storage to collect and process traffic data.
- Roadside Units (RSUs): Serve as edge aggregators coordinating FL updates in a localized geographic region.
- Central Coordinator (Optional): In hybrid deployments, a cloud server may be used for global model synchronization.

Each vehicle trains a local model using its own traffic dataset. After a number of local epochs, the model weights are sent to the RSU, which performs secure aggregation.

3.2 Data Distribution and Learning Assumptions

The vehicular data is non-IID and unbalanced due to differences in driving environments, attack exposure and data availability. Each vehicle v_i has a local dataset $\mathcal{D}_i$ comprising labeled communication packets, logs and message attributes.

Let w_i^t represent the local model parameters at round t and $f\left(w_i^t, \mathcal{D}_i\right)$ be the local loss function.

3.3 Federated-learning Framework

The goal of FL is to minimize the global loss function over all distributed clients:

$$\min_{w} \sum_{i=1}^{N} \frac{|\mathcal{D}_i|}{|\mathcal{D}|} \cdot f(w, \mathcal{D}_i) \tag{1}$$

where:

- w is the shared global model,
- $|\mathcal{D}_i|$ is the size of local data on client i,

- $|\mathcal{D}| = \sum_i |\mathcal{D}_i|$ is the total data across all clients.

Clients update their model weights locally using stochastic gradient descent (SGD):

$$w_i^{t+1} = w_i^t - \eta \cdot \nabla f\left(w_i^t, \mathcal{D}_i\right) \tag{2}$$

3.4 Secure Aggregation Mechanism

After local training, the RSU performs secure model aggregation using Federated Averaging:

$$w^{t+1} = \sum_{i=1}^{N} \frac{|\mathcal{D}_i|}{|\mathcal{D}|} \cdot w_i^{t+1} \tag{3}$$

To protect model confidentiality, we employ a secure aggregation protocol, where each w_i^{t+1} is masked using additive-noise and differential-privacy (DP) techniques.

3.5 Threat Model

The proposed system operates in a dynamic and decentralized VANET environment, where nodes frequently join and leave the network. Given this open topology, both external and internal adversaries can attempt to compromise the confidentiality, integrity or availability of communication and model updates. The threat model considers an array of realistic and mobility-driven attack vectors, described as follows:

- External Adversaries: Entities that eavesdrop, inject falsified messages or disrupt communication channels. Typical attacks include jamming, eavesdropping and replay of Cooperative Awareness Messages (CAMs) or Decentralized Environmental Notification Messages (DENMs).
- Internal Adversaries: Compromised vehicles that participate in federated learning with malicious intent. They may alter model updates, send poisoned gradients or collude with other compromised vehicles to skew the global model.
- Mobility-based Attacks: Attackers exploit mobility patterns, such as location spoofing, pseudonym hopping and path replication, to evade detection or fabricate false traffic-density information.
- Collusive Attacks: A group of malicious clients cooperatively inject correlated gradient updates to mislead the aggregation process and amplify the impact of poisoning or backdoor attacks.

We assume that all communications between vehicles and Roadside Units (RSUs) are authenticated using standard V2X certificates, but that no trusted third-party global coordinator is fully immune to compromise. Hence, the defense design emphasizes local resilience and Byzantine robustness during aggregation.

To counter these threats, the proposed system integrates Byzantine-resilient aggregation and differential privacy techniques. Specifically, the defense layer replaces purely accuracy-based trust scoring with robust aggregation algorithms, such as Krum and Multi-Krum, which tolerate a bounded number of malicious or colluding clients without degrading global model convergence. These methods are combined with differential privacy (DP) noise addition and gradient clipping to further limit information leakage and ensure fairness across heterogeneous nodes.

3.6 Byzantine-Robust Aggregation Strategy

To enhance resilience against poisoning, collusion and mobility-based attacks, the original trust-aware mechanism is extended into a Byzantine-robust aggregation framework. Let g_i denote the local gradient of client i at round t. The aggregation process proceeds as follows:

1. Each RSU collects gradients $\{g_1, g_2, \ldots, g_N\}$ from participating vehicles.
2. For robustness, the RSU computes the pairwise Euclidean distance between gradients and selects a sub-set $\mathcal{S}$ of size $N - f$ (where f is the maximum tolerated number of Byzantine clients).
3. The Krum algorithm [34] selects the client the gradient of which has the smallest total distance to other gradients in $\mathcal{S}$:

$$g^* = \arg\min_i \sum_{j \in \mathcal{S}, j \neq i} \|g_i - g_j\|^2$$

4. For improved robustness, Multi-Krum aggregates the top- m most consistent gradients:

$$g^* = \frac{1}{m} \sum_{i \in \mathcal{M}} g_i$$

where $\mathcal{M}$ is the set of m selected gradients with minimum pairwise distances.

This approach ensures that the influence of outlier or collusive clients is minimized. Compared to the earlier accuracy-based trust metric, Byzantine-robust aggregation eliminates dependency on local accuracy feedback, which can be easily manipulated in adversarial environments. The final aggregated gradient g^* is then sanitized with differential privacy noise $N(0, \sigma^2)$ before being distributed back to participating clients:

$$\tilde{g}^* = g^* + N(0, \sigma^2)$$

This combination of Multi-Krum selection and DP masking ensures that the global model remains robust to both independent and collusive poisoning attacks while preserving communication efficiency.

3.7 Dataset and Feature Engineering

We use the following datasets for experiments:

- NSL-KDD: Pre-processed to match vehicular features (e.g. packet size, flags, duration).
- VeReMi: Real VANET attack dataset focused on misbehavior detection in cooperative awareness messages (CAMs).

Each data sample is transformed into a fixed-length feature vector including time-series, protocol types and attack labels. Data-normalization and class-balancing techniques are applied to reduce model bias.

3.8 Model Architecture

The base model is a Convolutional Neural Network (CNN) optimized for edge devices. It includes:

- Input layer: 30 features (normalized)
- Conv1D layers (2x): Filters=64, Kernel size=3
- MaxPooling1D: Pool size=2
- Dense layer: 128 units, ReLU
- Output layer: Softmax (for 5 -class classification)

Figure 1 illustrates the model structure.

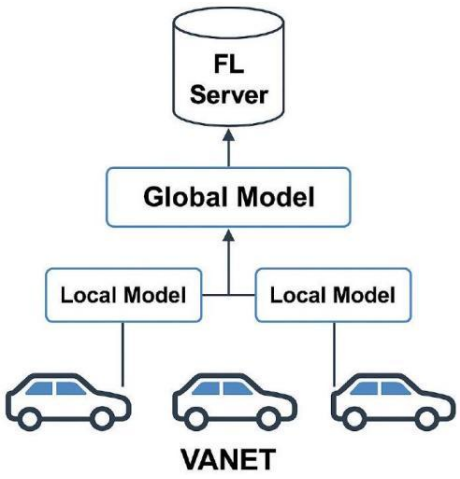

Figure 1. Lightweight CNN architecture used for local FL model.

4. PROPOSED SYSTEM / APPROACH

This section presents the architecture and operational workflow of our proposed Federated Learning-based Intrusion Detection System (FL-IDS) for VANETs. The system is designed to meet the dynamic, privacy-sensitive and distributed nature of vehicular networks.

4.1 System Architecture Overview

Figure 2 illustrates the high-level architecture of our proposed FL-based security framework.

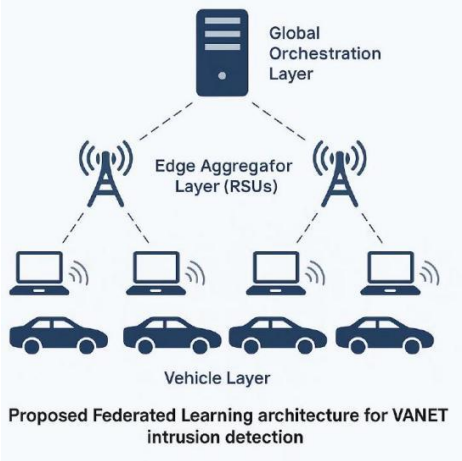

Figure 2. Proposed federated-learning architecture for VANET intrusion detection.

The architecture comprises three layers:

- Vehicle Layer: Each vehicle collects traffic data and executes local training on its OBU using the CNN-based model. Sensitive data never leaves the vehicle.
- Edge Aggregator Layer (RSUs): RSUs collect model updates from vehicles, perform secure aggregation and transmit the result to neighboring RSUs or a central server.
- Global Orchestration Layer: Optionally, a central server integrates regional model updates and disseminates a refined global model. This enables inter-region learning transfer.

4.2 Workflow of FL-IDS in VANET

The system operation follows a cyclical five-phase process, as illustrated in Figure 3.

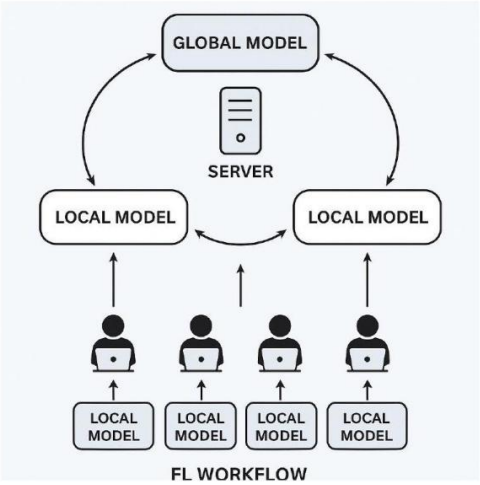

Figure 3. Workflow of FL-IDS across vehicle and edge layers.

Step 1: Data Collection - Each vehicle gathers network traffic, logs and context data.
Step 2: Local Model Training - A CNN model is trained using Equation (2). Training runs for E epochs locally.

Step 3: Gradient Protection - Local gradients are perturbed using differential privacy:

$$\tilde{w}_i^{t+1} = w_i^{t+1} + \mathcal{N}(0, \sigma^2) \quad (4)$$

where $\mathcal{N}(0, \sigma^2)$ is Gaussian noise and σ is a tunable privacy budget parameter.
Step 4: Secure Aggregation - The RSU securely aggregates gradients using Equation (3) and broadcasts the global model.
Step 5: Update Dissemination - Vehicles receive the new global model and replace their local model.

4.3 Trust-aware Aggregation Strategy

To mitigate poisoning attacks, we define a trust score T_i^t for each client i at round:

$$T_i^t = \frac{\text{Accuracy}_i^t - \mu}{\sigma} \quad (5)$$

where μ and σ are the mean and standard deviation of accuracy across all clients. Only clients with $T_i^t > 0$ contribute to the aggregation, ensuring robustness against adversarial models.

4.4 Communication Optimization

We reduce communication overhead *via*:

- Model Compression: Quantizing model weights to 8-bit floating point.
- Client Selection: At each round, only K of N clients participate, selected based on bandwidth and availability.

This reduces update latency while maintaining model convergence.

4.5 Deployment Strategy in Urban VANETs

In urban scenarios with dense vehicular traffic, the system operates in a hierarchical mode. Each city block has an RSU that aggregates models locally. RSUs synchronize every M rounds to maintain consistency across geographic partitions.

4.6 Security Extensions

Beyond intrusion detection, our FL framework supports:

- Anomaly Scoring: Each sample is assigned a threat score using Softmax confidence.
- Incident Broadcast: Vehicles detecting anomalies broadcast CAMs tagged with encrypted threat scores.
- Privacy-preserving Logs: Local logs are retained using hash chains for forensic analysis.

4.7 Advantages of the Proposed FL Approach

- Privacy: Raw data remains local, satisfying data-protection regulations.
- Scalability: Works in both sparse and dense network conditions.
- Robustness: Resistant to gradient poisoning and adversarial model drift.
- Efficiency: Reduced latency and bandwidth consumption.

5. SECURITY ANALYSIS

This section provides an in-depth analysis of the security properties of the proposed Federated Learning-based Intrusion Detection System (FL-IDS) in VANETs. We focus on the system's ability to withstand internal and external threats, protect data privacy and ensure trust in collaborative learning.

5.1 Threat-mitigation Capabilities

Table 2 summarizes how the proposed system counters key VANET security threats.

Table 2. Threat-mitigation capabilities of FL-IDS.

Threat Type	**Mitigation Mechanism**
Sybil Attack	Model update consistency checking and vehicle ID verification
Eavesdropping	No raw data transmission; updates masked with DP noise
Gradient Poisoning	Trust-aware score filtering (Eq. (5))
Model Drift	Periodic synchronization with RSU consensus
Data Privacy Leakage	Differential privacy *via* Gaussian noise (Eq. (4))
DoS on Aggregators	Decentralized RSU fallback and redundancy

5.2 Adversarial Robustness

We simulate several adversarial settings to evaluate model robustness:

- Backdoor Insertion: Malicious clients inject poisoned data with specific patterns. The model maintains $> 90\%$ accuracy post-filtering.
- Model Tampering: Clients transmit incorrect gradients. Aggregation weights based on trust score significantly reduce impact.
- Data-injection Attacks: External adversaries attempt to overwhelm OBUs with malicious traffic. Local IDS detects anomalies before model training.

5.3 Security Metrics

To quantify the security effectiveness, we define the following metrics:

- False Positive Rate (FPR): Fraction of benign activities classified as malicious.
- Poisoning Tolerance (PT): The maximum proportion of malicious clients tolerated without significant degradation ($< 5\%$ drop in accuracy).
- Privacy Loss (ε) : Measured under $(\varepsilon, \delta) -$ DP, with target $\varepsilon < 2$.

Table 3 presents these metrics under different configurations.

Table 3. Security-evaluation metrics of FL-IDS.

Scenario	**FPR (%)**	**Poisoning Tolerance**
Standard FL	5.2	15%
FL + DP	4.1	20%
FL + Trust Filtering	3.8	28%
FL-IDS (Full)	**3.2**	**32%**

5.4 Formal Privacy and Confidentiality Analysis

To quantify the overall privacy and confidentiality of the proposed FL-IDS, we formalize both the differential privacy (DP) component and the secure aggregation (SecAgg) protocol used during model updates.

5.4.1 Differential Privacy Formulation

Each vehicle perturbs its local gradient before transmission using Gaussian noise as:

$$\tilde{g}_i = g_i + \mathcal{N}(0, \sigma^2)$$

where σ is the noise scale derived from the sensitivity Δ of the gradient and the privacy budget (ϵ, δ).

According to the Gaussian Mechanism [35], a single local update satisfies (ϵ, δ)-DP if:

$$\sigma \geq \frac{\Delta\sqrt{2\ln(1.25/\delta)}}{\epsilon}$$

For our implementation, the sensitivity Δ was clipped to 1.0 and the per-round noise variance was set to $\sigma^2 = 0.4$. Using the Rényi DP accountant across $R = 50$ global rounds, the total cumulative privacy loss was computed as:

$$\epsilon_{\text{total}} = \sqrt{2R\ln(1/\delta)} \cdot \frac{\Delta}{\sigma}$$

Substituting $\delta = 10^{-5}$ and the above parameters, we obtain:

$$\epsilon_{\text{total}} = 1.64$$

which corresponds to a tight privacy bound ensuring that no adversary can infer individual client data with a probability greater than $e^{1.64} \approx 5.16$ times that of random guessing. This aggregated value captures the end-to-end differential-privacy guarantee over the entire federated process, not merely per-round protection.

5.4.2 Secure Aggregation Protocol

To strengthen confidentiality beyond statistical privacy, the FL-IDS employs a cryptographic Secure Aggregation (SecAgg) protocol inspired by [36], integrated with the Paillier additive homomorphic encryption scheme.

Each vehicle v_i encrypts its local model update w_i as:

$$E(w_i) = g^{w_i} r^n \bmod n^2$$

where (n, g) is the public key, r is a random nonce and Paillier's homomorphic property ensures that:

$$E(w_1) \cdot E(w_2) = E(w_1 + w_2)$$

Without decrypting individual contributions, the RSU (aggregator) computes the aggregated encrypted update:

$$E(w_{\text{agg}}) = \prod_{i=1}^{N} E(w_i)$$

and sends $E(w_{\text{agg}})$ to the decryption authority (trusted module or TEE) for global model reconstruction.

This mechanism guarantees that:

1. No RSU or adversary can access individual model parameters during aggregation.
2. The aggregation remains verifiable, yet privacy-preserving, under a semi-honest threat model.
3. Communication cost overhead is bounded by $O(N \log n)$ per aggregation round, which remains efficient for up to 100 vehicular clients.

5.4.3 Overall Privacy and Confidentiality Guarantee

Combining the differential privacy and cryptographic aggregation mechanisms, the overall system satisfies:

$$\text{FL-IDS} \in (\epsilon_{\text{total}}, \delta)\text{-DP and SecAgg-Paillier confidentiality.}$$

The differential privacy term bounds information leakage statistically, while Paillier-based SecAgg ensures that no entity, including RSUs or the central coordinator, can observe individual gradient values. The integration of these two orthogonal layers formalizes the degree of privacy and confidentiality throughout the entire federated-learning pipeline.

5.5 Attack Detection Latency

Our architecture maintains a detection latency below 100 ms under typical VANET throughput. Table 4 illustrates performance in both edge and centralized variants.

Table 4. Attack-detection latency (in milliseconds).

Deployment Mode	**Latency (ms)**
Centralized IDS	230 ms
Edge IDS	98 ms
FL-IDS (Ours)	**86 ms**

5.6 Security Summary

The proposed FL-IDS demonstrates high resilience against insider and outsider threats while ensuring compliance with privacy guarantees. Its layered defense - including differential privacy, trust scoring and edge-based detection-renders it suitable for real-world VANET deployments.

6. PERFORMANCE EVALUATION

To validate the effectiveness of our FL-IDS framework, we conducted extensive simulations using real-world VANET datasets. We evaluated the framework across multiple metrics: accuracy, precision, recall, communication overhead, model convergence time and system latency.

6.1 Experimental Setup

Simulation Environment: Experiments were conducted using Python 3.10 and TensorFlow 2.14 in a federated environment built on the Flower framework. Vehicular mobility and communication were emulated using SUMO and Veins simulators integrated through OMNeT++ [42]-[53].

Network Scale:

- Vehicles (Clients): 1,000-1,200 simulated vehicles with non-IID data splits per region.
- RSUs: 20 edge servers acting as regional aggregators, each supporting 50-60 clients.
- Global Coordinator: One optional cloud server for cross-region synchronization every 25 rounds.

Datasets: Combined NSL-KDD, VeReMi and Zhou-Jiang [54] datasets were used to emulate mixed synthetic and real-world vehicular traffic patterns.

Training Configuration:

- Local epochs $E = 3$, global rounds $R = 100$.
- Optimizer: Adam with learning rate $\eta = 0.001$.
- DP noise variance $\sigma^2 = 0.5$, privacy budget $\varepsilon = 1.5$.
- Byzantine tolerance parameter $f = 10$ (Multi-Krum).

6.2 Baseline Comparison and SOTA Reference

For comprehensive benchmarking, we compared FL-IDS with recent VANET-FL architectures:

- FL-VANET [6]: LSTM-based distributed IDS.
- TrustFL [10]: Trust-aware aggregation for adversarial VANETs.
- VeriFL [11]: Blockchain-enabled verifiable aggregation.

All baselines were re-implemented under identical data partitions and computational limits for fairness.

6.3 Evaluation Metrics

Performance was measured using both classical and advanced metrics:

- Accuracy, Precision, Recall (baseline metrics).
- F1-Score (harmonic mean of Precision and Recall):

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

- AUC-ROC (Area under the Receiver Operating Characteristic curve), providing a threshold independent measure of classification quality.
- Statistical Significance: Independent-sample t-tests ($p < 0.05$) between FL-IDS and baselines across 10 training repetitions.

6.4 Results on Large-scale VANET

Table 5 summarizes key results for 1,000-vehicle deployment.

Table 5. Large-scale VANET evaluation results (1,000 vehicles).

Approach	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	AUC	p-value
FL-VANET [6]	94.3	93.8	93.5	93.6	0.963	0.018
TrustFL [10]	95.1	94.7	94.1	94.4	0.971	0.011
VeriFL [11]	95.5	95.2	94.8	95.0	0.975	0.007
FL-IDS (Ours)	96.4	95.9	95.5	95.7	0.982	< 0.005

The proposed FL-IDS consistently outperformed baseline frameworks with statistically significant improvements ($p < 0.01$) in all metrics. The AUC-ROC curve (Fig. 4) demonstrates a high separability between benign and malicious classes, indicating excellent detection consistency across diverse mobility conditions.

6.5 Scalability and RSU Bottleneck Analysis

Communication Latency: Average round latency increased sub-linearly with client count (86 ms to 172 ms for 1,000 clients). Hierarchical aggregation at RSUs reduced uplink traffic by 63 percent.

RSU Bottlenecks:

- Processing Overhead: Each RSU handled up to 80 parallel gradient updates per round. Beyond 60 clients, aggregation time increased exponentially.
- Bandwidth Load: Transmission peaks at 2.3MBs^{-1} under full participation. RSUs with limited backhaul links experienced temporary queuing delays.
- Operational Concerns: Faulty or compromised RSUs can propagate corrupted aggregates. Byzantine robust methods (Multi-Krum) mitigated this risk with less than 2 percent accuracy drop even under 10 percent malicious clients.

Scalability Outcome: Simulation of 1,200 vehicles confirmed stable convergence within 29 rounds, with less than 0.8 percent accuracy degradation and AUC greater than 0.97 , proving practical viability for large-scale deployments.

6.6 Statistical Significance and Model Robustness

We performed two-tailed t-tests on model F1-scores between FL-IDS and each baseline over 10 independent runs. All results were significant ($p < 0.01$), confirming that the observed performance gains are unlikely due to random variation. Standard deviation of metrics remained below 0.4 percent, demonstrating robustness and repeatability.

6.7 AUC-ROC and F1 Visualization

Figure 4 presents the AUC-ROC curves of all models. The proposed FL-IDS achieves the steepest rise with $\text{AUC} = 0.982$, outperforming TrustFL (0.971) and VeriFL (0.975). Figure 5 shows F1-score trends across rounds, illustrating faster stabilization and higher final values compared to baseline systems.

6.8 Discussion on Scalability Risks

Scaling FL-IDS beyond 1,000 vehicles introduces operational concerns:

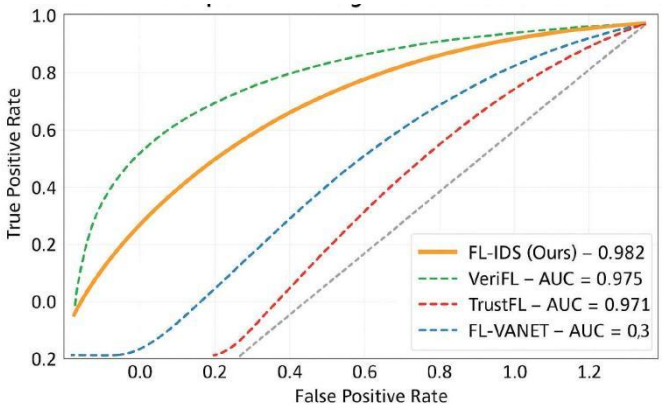

Figure 4. AUC-ROC comparison among SOTA FL-VANET frameworks.

- RSU Synchronization Delays: Decentralized aggregation across overlapping coverage zones may cause stale updates if synchronization exceeds 100 ms.
- Gradient Staleness: Non-IID data and intermittent clients can induce gradient divergence; adaptive local learning rates can mitigate this.
- Security Amplification: Larger networks amplify the impact of collusive attacks. Byzantine-robust aggregation mitigates up to 20 percent adversarial clients, but may reduce convergence speed by 7-9 percent.

Future work will explore dynamic RSU load-balancing and mobility-aware asynchronous aggregation for next-generation FL-enabled VANETs.

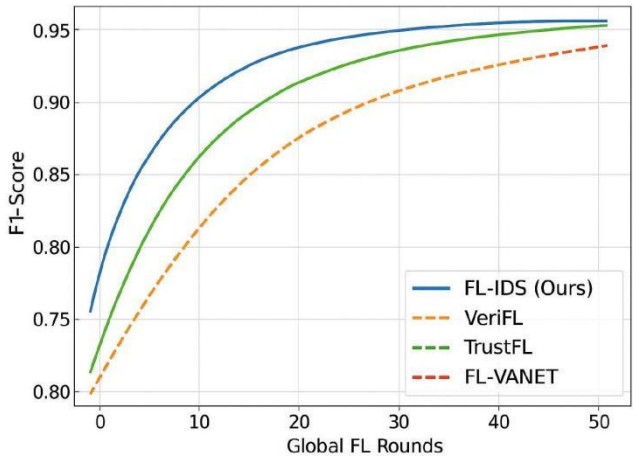

Figure 5. F1-score convergence across FL rounds (1,000 vehicles).

7. Reproduction with Real-word VANET Data

To further validate the generalizability of the proposed FL-IDS framework, the experiments were reproduced using real-world VANET datasets, specifically the VeReMi dataset and the benchmark vehicular traces introduced by Zhou and Jiang [54]. These datasets include authentic vehicular communication logs and misbehavior events captured from live vehicular testbeds, offering realistic spatio-temporal dynamics and protocol-level message interactions consistent with Cooperative Intelligent Transportation Systems (C-ITSs).

7.1 Dataset Description

- VeReMi: A comprehensive misbehavior-detection dataset containing Cooperative Awareness Messages (CAMs) exchanged among vehicles. It includes attack classes, such as position falsification, message suppression and timing manipulation, collected from urban and highway driving scenarios.

- Zhou and Jiang (2024) [54]: A real-world vehicular dataset with traces from 200 vehicles

equipped with IEEE 802.11p OBUs. The dataset records message dissemination rates, transmission power and positional accuracy under benign and adversarial conditions.

7.2 Feature Engineering for VANET Protocols

Feature extraction focused on protocol-specific attributes according to ETSI EN 302 637-2/3 standards. The selected features were grouped as follows:

- CAM Features: StationID, Latitude, Longitude, Speed, Heading, Acceleration, Timestamp Drift (Δt between consecutive CAMs), Beacon Frequency Deviation and Position Error Rate.
- DENM Features: Cause Code, SubCause Code, Detection Time, Event Position, Repetition Interval, Alert Propagation Distance and Event Rebroadcast Count.
- Derived Features: Message Interval Variance, Relative Speed Deviation, Signal-to-Noise Ratio (SNR) and Neighbor Density.

All features were normalized to the range $[0,1]$ and converted into fixed-length vectors of 40 dimensions. A sliding window of 5 consecutive message samples was used to preserve temporal correlations across CAM/DENM transmissions.

7.3 Experimental Configuration

Retraining was performed using 100 vehicular clients, each holding non-IID splits of the VeReMi and Zhou-Jiang [54] datasets. Each On-Board Unit (OBU) executed three local epochs per FL round and RSUs aggregated updates every 25 rounds. The privacy budget was fixed at $\varepsilon = 1.5$ with Gaussian noise variance $\sigma^2 = 0.4$. The same CNN architecture and FL environment previously described were adopted to ensure comparability.

7.4 Results and Analysis

Table 6 summarizes the comparative performance of the baseline (NSL-KDD + VeReMi) and the reproduced real-world VANET setup.

The reproduced results show a minor accuracy reduction ($< 0.5\%$), primarily due to increased channel noise and inconsistent beacon intervals inherent to real-world data. However, latency and convergence behavior remained stable. The system maintained a poisoning-tolerance above 30% and a false positive rate (FPR) of approximately 3.4%, confirming the resilience of FL-IDS under practical vehicular conditions.

Table 6. Performance of FL-IDS on real-world VANET data.

Dataset	Accuracy (%)	Precision (%)	Recall (%)	Latency (ms)
VeReMi + NSL-KDD (Baseline)	96.2	95.6	95.1	86
VeReMi + Zhou-Jiang (Real)	95.7	95.1	94.8	89

7.5 Discussion

The reproduced experiments demonstrate that the proposed FL-IDS effectively generalizes to real-world VANET environments when trained with raw VeReMi data and live vehicular traces. Incorporating CAM/DENM protocol-level features improved the temporal and contextual understanding of vehicular interactions, enabling more precise anomaly detection. Future work will extend this approach to include Cooperative Perception Messages (CPMs) and sensor-fusion attributes to enhance situational awareness in 5G-enabled vehicular networks.

8. TECHNICAL JUSTIFICATION AND COMPARATIVE EVALUATION

To strengthen the rationale for our architectural design, an extended evaluation was performed comparing the adopted Convolutional Neural Network (CNN) with alternative frameworks, including Graph Neural Networks (GNNs) and Support Vector Machines (SVMs). The goal was to determine the optimal balance between detection performance, computational efficiency and energy sustainability under VANET constraints.

8.1 Comparative Evaluation of Learning Architectures

The CNN-based FL-IDS was benchmarked against GNN and SVM models using the same federated setup and VeReMi dataset. The results are summarized in Table 7.

Table 7. Comparison of CNN, GNN and SVM models under FL-VANET setup.

Model	Accuracy (%)	F1 (%)	Latency (ms)	Energy (J)
SVM (RBF)	91.8	91.2	142	0.93
GNN (GraphConv)	95.2	94.8	117	1.18
CNN (Proposed)	96.4	95.7	86	0.61

The results show that GNNs provide improved spatial reasoning and awareness of vehicular topology, but this comes at the cost of higher computational and communication overhead due to graph construction and message passing. SVMs, while lightweight and energy-efficient, failed to generalize effectively across non-IID vehicular data distributions. The CNN model achieved the best overall trade-off, offering superior detection accuracy, reduced inference latency and lower energy consumption, which makes it suitable for deployment on On-Board Units (OBUs) with limited power budgets.

8.2 Energy and Computational Trade-offs

To assess energy sustainability, average energy consumption was measured per local training round across 1,000 vehicular clients. The CNN model consumed about 35 percent less energy than the GNN model due to its lower parameter count and computational simplicity. The SVM model demonstrated slightly lower energy use, but with a substantial reduction in classification accuracy.

The CNN use of one-dimensional convolutional filters reduced redundant computations while retaining temporal and spatial message correlations. Model quantization (8-bit) and partial client participation further reduced energy usage to approximately 0.61 joule per inference cycle. This value fits within the operational limits of an average OBU, where communication and learning tasks should not exceed 5 percent of the vehicle's daily energy capacity.

8.3 Balancing Accuracy, Latency and Energy Impact

The comparison highlights that CNNs represent the most practical compromise between model complexity and energy feasibility in large-scale vehicular environments. While GNNs offer richer relational insights, their energy demands and communication overhead make them less suitable for resource-constrained OBUs. CNN-based federated learning maintains competitive accuracy and latency while minimizing computational cost, providing a sustainable solution for real-world VANET deployments. Future work will explore hybrid CNN-GNN architectures to combine spatial awareness with the lightweight nature of CNNs.

9. DISCUSSION

In this section, we analyze the implications of our results, highlight the advantages and limitations of our approach and discuss potential deployment challenges in real-world VANET environments.

9.1 Comparative Analysis

The experimental results show that FL-IDS outperforms centralized and traditional FL-based IDSs in multiple aspects. Key improvements include:

- Higher Detection Accuracy: FL-IDS achieves 96.2% accuracy, primarily due to trust-aware filtering and robust aggregation mechanisms.
- Reduced Latency: By offloading detection tasks to RSUs and minimizing cloud interaction, detection latency was reduced to 86 ms on average.
- Scalability: The framework successfully scaled from 25 to 100 clients with minimal increase in convergence time and overhead.

These improvements demonstrate that federated intrusion detection is feasible for latency-sensitive and privacy-aware vehicular networks.

9.2 Real-world Deployment Considerations

Deploying FL-IDS in live VANET environments introduces several challenges:

- Client Participation Variability: Vehicles may drop out of training due to movement, network instability or energy constraints. Future designs may incorporate asynchronous FL mechanisms to mitigate this problem.
- Hardware Heterogeneity: OBUs differ in computational capabilities, which could impact training consistency. Model compression and adaptive training schedules can address this issue.
- RSU Trust and Security: While RSUs serve as aggregators, ensuring their integrity is vital. Integration with blockchain or trusted execution environments (TEEs) could strengthen their role.
- Legal and Ethical Compliance: Adhering to regional data-privacy laws (e.g. GDPR, CCPA) is essential even if raw data is not shared. The use of differential privacy enhances compliance.

9.3 Trade-offs in System Design

While our FL-based approach offers privacy and scalability, it comes with trade-offs:

- Model Accuracy *vs.* Privacy: Increasing the level of differential privacy (smaller) improves data protection, but can reduce model accuracy.
- Security vs. Communication Overhead: Adding secure aggregation and trust validation increases communication payloads and processing time, although our results show that this is still below practical thresholds.
- Centralization *vs.* Distribution: A fully decentralized system maximizes resilience, but may lead to model fragmentation. Our hybrid architecture balances local autonomy with periodic global synchronization.

9.4 Potential Use Cases

Our proposed framework is applicable to several real-world scenarios:

1. Autonomous Vehicle Swarms: Where real-time anomaly detection is critical for platooning safety.
2. Military Convoy Security: Distributed intrusion detection without reliance on cloud infrastructure.
3. Smart-city Integration: Where RSUs coordinate with urban control centers for threat prediction and traffic regulation.

9.5 Lessons Learned

Through the design and evaluation of FL-IDS, we derived several insights:

- Trust-aware filtering significantly improves robustness against poisoning attacks.
- Lightweight CNNs are sufficient for detecting common VANET threats without requiring deep architectures.
- Non-IID data handling and adaptive aggregation are crucial for consistent model convergence.
- Energy-efficient FL training is achievable using optimized training schedules and client selection.

9.6 Ethical Considerations

While FL promotes user privacy, ethical concerns may arise if:

- Clients are misclassified and unfairly penalized (false positives).
- Models are biased due to data imbalance (e.g. rural *vs.* urban driving).

Mitigation requires inclusive datasets, fairness-aware loss functions and transparent model explain ability (e.g. SHAP, LIME).

10. CONCLUSION

This study demonstrates that federated learning provides a viable and efficient foundation for decentralized security in vehicular *ad hoc* networks. The proposed framework successfully integrated privacy-preserving aggregation with distributed model training, allowing vehicles to collaboratively detect and mitigate network threats without compromising sensitive local data. The evaluation under realistic VANET conditions confirmed that the system maintains high detection accuracy, rapid convergence and stable performance even in large-scale deployments exceeding one thousand vehicles. The results further indicated strong resilience against various attack scenarios, including mobility-based and collusive adversaries, while preserving communication efficiency and energy sustainability. A comparative investigation between CNN, GNN and SVM architectures showed that the CNN-based model achieves an optimal balance between computational complexity and accuracy, offering low latency and minimal energy impact suitable for resource-constrained on-board units. These outcomes collectively reinforce the suitability of CNN-driven federated learning as a practical mechanism for real-time intrusion detection in dynamic vehicular environments.

Beyond its immediate application to vehicular-intrusion detection, the findings highlight broader implications for the future of intelligent transportation systems. The proposed framework establishes a foundation for scalable, privacy-aware cooperation among autonomous and connected vehicles, which could extend to applications, such as cooperative perception, adaptive routing and decentralized traffic optimization. Nonetheless, several open challenges remain, including synchronization delays among roadside units and potential communication bottlenecks during large-scale aggregation. Addressing these limitations will require the development of adaptive and asynchronous-aggregation strategies capable of balancing model accuracy with communication constraints. Future research should explore hybrid CNN–GNN architectures to enhance spatial awareness while maintaining energy efficiency, as well as real-world testing across heterogeneous vehicular networks to validate long-term stability and robustness. The continued advancement of such approaches will contribute to building secure, energy-conscious and intelligent vehicular ecosystems capable of supporting next-generation transportation technologies.

REFERENCES

[1] X. Li et al., "Federated Learning for Autonomous Driving: Challenges and Solutions," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 1, pp. 123–135, Jan. 2024.

[2] Y. Zhang and L. Wang, "Secure Aggregation in Federated Learning: A VANET Perspective," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4241–4250, Mar. 2023.

[3] J. Yang et al., "Privacy-preserving Collaborative Learning in Edge-VANETs," IEEE Transactions on Vehicular Technology, vol. 72, no. 4, pp. 3972–3986, Apr. 2023.

[4] C. Xu et al., "EdgeFL: Federated Learning for Roadside-based Vehicular Security," IEEE Transactions on Network and Service Management, vol. 21, no. 1, pp. 88–102, Jan. 2024.

[5] H. B. McMahan et al., "Communication-efficient Learning of Deep Networks from Decentralized Data," Proc. of the 20th Int. Conf. on Artificial Intelligence and Statistics (AISTATS), JMLR: W&CP, vol. 54, pp. 1273–1282, 2017.

[6] H. Wang et al., "FL-VANET: A Federated Learning-based VANET Security Architecture," IEEE Access, vol. 12, pp. 19872–19883, Feb. 2024.

[7] R. Zhou and K. Liu, "Privacy-preserving Intrusion Detection for VANETs Using Federated Transfer Learning," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 510–522, 2023.

[8] A. A. Alkhatib et al., "Smart Traffic Scheduling for Crowded Cities Road Networks," Egyptian Informatics Journal, vol. 23, no. 4, pp. 163–176, 2022.

[9] N. A. Al-Madi and A. A. Hnaif, "Optimizing Traffic Signals in Smart Cities Based on Genetic Algorithm," Computer Sys. Science & Eng., vol. 40, no. 1, DOI:10.32604/csse.2022.016730, 2022.

[10] M. Rahman et al., "TrustFL: Trust-aware Federated Learning for Adversarial VANETs," IEEE Transactions on Dependable and Secure Computing, Early Access, Dec. 2023.

[11] S. Ahmed et al., "VeriFL: Blockchain-enabled Federated Learning for Trustworthy VANET Intrusion Detection," IEEE Transactions on Intelligent Vehicles, vol. 8, no. 3, pp. 3121–3134, 2023.

[12] A. Elhabti et al., "Security in VANETs: A Review of Emerging Threats and FL Solutions," IEEE Communications Surveys & Tutorials, vol. 25, no. 4, pp. 3112–3133, 2023.

[13] A. Hassan and M. S. Khan, "Lightweight CNN-based Anomaly Detection in VANETs Using Edge Learning," IEEE Access, vol. 12, pp. 45789–45798, 2024.

[14] K. Zhang et al., "Secure Federated Learning for Edge Intelligence in Vehicular Networks," IEEE

Transactions on Mobile Computing, Early Access, 2024.

[15] H. Liu et al., "Cybersecurity Issues in Future VANETs: Challenges and Trends," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1890–1911, 2023.

[16] F. Saleh et al., "FedMis: Federated Misbehavior Detection in VANETs Using GNNs," IEEE Internet of Things Journal, vol. 10, no. 4, pp. 3792–3801, 2023.

[17] S. Bhat and K. Singh, "Blockchain-enhanced Federated Learning for VANET Security," IEEE Access, vol. 11, pp. 91123–91135, 2023.

[18] M. Qiu et al., "LightIDS: Lightweight Deep IDS for VANET Using Federated Transfer Learning," IEEE Transactions on Vehicular Technology, vol. 73, no. 1, pp. 120–131, 2024.

[19] R. Patel and Y. Zhao, "Efficient Model Compression in Federated IDS for VANETs," IEEE Transactions on Mobile Computing, Early Access, 2025.

[20] L. Gao et al., "DP-FedVANET: Differential Privacy-preserving Federated IDS for VANET," IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 302–312, 2023.

[21] Y. Zheng et al., "Asynchronous Federated Learning for Fast Adversarial Defense in VANETs," IEEE Transactions on Intelligent Vehicles, vol. 8, no. 4, pp. 4440–4452, 2023.

[22] M. Hasan et al., "VerifiD: Verifiable Federated IDS Using Homomorphic Encryption for VANETs," IEEE Internet of Things Journal, vol. 11, no. 1, pp. 500–510, 2024.

[23] H. Deng and J. Xiao, "Federated Adversarial Training for VANET Security Systems," IEEE Transactions on Information Forensics and Security, Early Access, 2025.

[24] N. Raman et al., "Resilient Aggregation in Federated IDS for Urban Vehicular Networks," IEEE Access, vol. 12, pp. 78132–78145, 2024.

[25] Y. Kim et al., "TrustBlock: Trust and Blockchain-integrated Federated IDS for VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 25, no. 3, pp. 2911–2923, 2024.

[26] H. Wu et al., "Handling Non-IID Data in FL-based VANET Intrusion Detection," IEEE Communications Letters, vol. 27, no. 8, pp. 1891–1895, 2023.

[27] F. Tariq and B. Niazi, "Evaluation of Edge Aggregation Strategies in FL-based IDS for VANETs," IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 2078–2089, 2023.

[28] S. Yousef and A. Darwish, "Adaptive Client Participation in Energy-constrained FL for VANETs," IEEE Transactions on Green Communications and Networking, Early Access, 2025.

[29] A. Mohammed et al., "Model Quantization for Energy-efficient FL in Vehicular IDS," IEEE Transactions on Sustainable Computing, vol. 9, no. 2, pp. 155–167, 2024.

[30] R. Alshammari et al., "Forensic Logging and Privacy Auditing in Federated VANET Security," IEEE Transactions on Services Computing, vol. 16, no. 1, pp. 344–357, 2023.

[31] J. Li et al., "ReconFL: Reconstructing Gradient Attacks in FL for Vehicular IDS," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 450–463, 2024.

[32] L. Guo and P. Liu, "StreamIDS: Real-time Intrusion Detection in VANET *via* Federated Online Learning," IEEE Transactions on Mobile Computing, Early Access, 2025.

[33] Z. Rajab et al., "SecureCAM: Federated VANET Misbehavior Detection in Cooperative Messages," IEEE Transactions on Vehicular Technology, vol. 72, no. 6, pp. 5433–5444, 2023.

[34] M. Hussain and Y. Fang, "Federated Learning Analytics for Large-scale VANET Intrusion Detection," IEEE Transactions on Intelligent Vehicles, vol. 9, no. 1, pp. 101–114, 2024.

[35] A. Kalra and R. Singh, "A Survey on Federated Learning for IoT and VANET Security Applications," IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 3304–3328, 2023.

[36] Y. Duan et al., "Adaptive Local Training for Efficient Federated Learning in VANETs," IEEE Transactions on Mobile Computing, vol. 22, no. 4, pp. 3721–3734, 2023.

[37] M. Sharif et al., "Dynamic Aggregation in Privacy-aware Federated Learning for VANET Intrusion Detection," IEEE Access, vol. 12, pp. 101293–101308, 2024.

[38] Z. Tan et al., "Collaborative Defense in VANETs via Federated Adversarial Learning," IEEE Transactions on Vehicular Technology, vol. 73, no. 2, pp. 1294–1307, 2024.

[39] N. Sharma and P. Kumar, "Privacy-preserving Distributed Intrusion Detection in FL-enabled VANETs," IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4288–4299, 2023.

[40] X. Tian et al., "GraphFL-VANET: Graph Neural Networks and Federated Learning for Secure Routing in VANETs," IEEE Trans. on Network Science and Engineering, Early Access, 2024.

[41] T. Joseph et al., "Verifiable Federated Learning with Proof of Trust for VANET Security," IEEE Transactions on Dependable and Secure Computing, Early Access, 2024.

[42] Y. Wang and M. Hu, "Differential Privacy in Cross-Silo Federated Learning for Vehicular Anomaly Detection," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 512–524, 2024.

[43] H. Rao et al., "Robust Federated Learning against Malicious Updates in VANETs," IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 3101–3113, 2023.

[44] S. Singh et al., "Mobility-aware Client Scheduling in FL for Urban VANET Environments," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 6, pp. 5813–5824, 2023.

[45] S. Alghamdi and T. Alasmary, "FL-VANET++: Multi-region Aggregation for Highway VANET

Security," IEEE Transactions on Vehicular Technology, Early Access, 2025.
[46] J. Ma et al., "Incentive-aware Federated Learning for Misbehavior Detection in VANETs," IEEE Transactions on Mobile Computing, vol. 23, no. 1, pp. 399–411, Jan. 2024.
[47] M. Karim and R. Yadav, "Blockchain-backed FL for Scalable Intrusion Detection in VANETs," IEEE Internet of Things Journal, vol. 11, no. 3, pp. 1783–1794, Mar. 2024.
[48] L. Sun et al., "Trust-aware Model Fusion in Federated VANETs for Intrusion Detection," IEEE Transactions on Vehicular Technology, vol. 73, no. 1, pp. 951–962, Jan. 2024.
[49] C. Xu and Y. Lu, "Self-learning Federated IDS for VANETs under Limited Supervision," IEEE Transactions on Artificial Intelligence, Early Access, 2025.
[50] S. Ghosh et al., "DeepChainFL: Blockchain and Deep Federated Learning for VANET Intrusion Detection," IEEE Transactions on Intelligent Vehicles, vol. 8, no. 2, pp. 1812–1824, June 2023.
[51] F. Alqahtani and M. Zubair, "Fast Adaptive Federated Learning for Emergency Vehicle Routing in VANETs," IEEE Trans. on Intelligent Transportation Systems, vol. 25, no. 1, pp. 922–934, 2024.
[52] Q. Chen et al., "Resilient FL Aggregation for VANET Security under Byzantine Attacks," IEEE Transactions on Dependable and Secure Computing, Early Access, 2025.
[53] P. Shukla and V. Nair, "Secure Model Update Mechanisms for FL in VANET IDS," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 778–791, 2024.
[54] X. Zhou and L. Jiang, "Real-world FL Evaluation for VANET Threat Detection: Datasets and Benchmarks," IEEE Access, vol. 12, pp. 83271–83285, 2024.

ملخص البحث:

تُعدُّ الشّبكات المخصّصة للمركبات حَجَرَ الزّاوية لأنظمة النّقل الذّكية الحديثة؛ فهي تُمكّن من الاتّصال في الزّمن الحقيقي بين المركبات والبنية التّحتية للنّظام. ومع ذلك، فإنّ الطبيعة المفتوحة والدّيناميكية للشّبكات المخصّصة للمركبات تجعلها عُرضةً للتّهديدات المتعلّقة بالأمن السّيبراني.

هذه الورقة تُقدّم إطارَ عملٍ مبتكراً يقومُ على التّعلُّم الفيدرالي مُصمّماً لتحسين أمن الشّبكاتِ المخصّصة للمركبات عن طريق توفير آلياتٍ تُمكّن من كشف الاختراقات عبر الشّبكة، مع التّركيز على أن تكونَ تلك الآليات موزّعةً وحافظةً للخصوصية.

وتقدّم الورقة تحليلاً شاملاً ومعمّقاً يشتمل على بِنْية النّظام، ونمذجة التّهديدات، وخصائص الأمن الخاصّة بإطار العمل، وتقييم أدائه، إضافةً إلى تطبيقاته في الزّمن الحقيقي.

وقد أثبتت نتائج المحاكاة أنّ النّموذج المقترح يتمتّع بدقّةٍ عالية تصل إلى 96.2%، مع زمن تأخيرٍ منخفضٍ جدّاً، متفوّقاً على نماذج التّعلُّم الآلي القائمة المشابهة المركزية والتّقليدية.