TrustV2X: A Hybrid Hierarchical and Transfer Federated Learning Framework for Trustworthy Next-Generation V2X Network Communication

Simeon Okechukwu Ajakwe*
ICT Convergence Research Centre
Kumoh National Institute of Technology
Gumi, Gyenongsangbuk, Republic of Korea
simeonajlove@gmail.com

Dong Seong Kim
IT Convergence Engineering Department
Kumoh National Institute of Technology
Gumi, Gyenongsangbuk, Republic of Korea
dskim@kumoh.ac.kr

Abstract

The increasing complexity of vehicular communication ecosystems, such as Vehicle-to-Everything (V2X) systems, introduces multifaceted cybersecurity challenges. While traditional intrusion detection systems (IDS) rely on centralized architectures, they fail to meet latency and privacy constraints of distributed vehicular networks. This paper presents TrustV2X, a novel hybrid Hierarchical Federated Learning (HFL) and Federated Transfer Learning (FTL) framework for V2X intrusion detection. The design integrates edge-level training cycles, transfer-phase adaptation schedules, and a rule-based client vetting mechanism to achieve privacy-preserving and intrusion-resilient learning at Roadside Units (RSUs) and Multi-access Edge Computing (MEC) aggregators. Experimental validation on the CICIoV2024 dataset demonstrates that the proposed framework achieves an F1-score of 100% and reduces training latency by 27.4% compared to conventional FL-based IDS models. The proposed hybrid architecture provides a scalable pathway for trustworthy and adaptive V2X security systems.

CCS Concepts

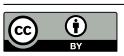
• ; • **Information systems**; • **Computing methodologies**; • **Security and privacy**;

Keywords

V2X, Intrusion Detection, Federated Learning, Hierarchical Federated Learning, Transfer Learning, Edge Intelligence, Vehicular Security

ACM Reference Format:
Simeon Okechukwu Ajakwe and Dong Seong Kim. 2025. TrustV2X: A Hybrid Hierarchical and Transfer Federated Learning Framework for Trustworthy Next-Generation V2X Network Communication. In *The 9th International Conference on Algorithms, Computing and Systems (ICACS 2025), December 12–14, 2025, Bangkok, Thailand*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3789418.3789443

*ICT Convergence Research Center, Kumoh National Institute of Technology, Gumi, South Korea



ICACS 2025, Bangkok, Thailand

ACM ISBN 979-8-4007-1961-5/25/12
https://doi.org/10.1145/3789418.3789443

1 Introduction

Emerging connected and autonomous vehicles rely heavily on Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), and broader Vehicle-to-Everything (V2X) communication to exchange safety-critical data [3]. However, the distributed nature of V2X networks increases the attack surface, rendering traditional centralized intrusion detection systems (IDS) ineffective due to high latency, privacy concerns, and scalability constraints. The explosive growth of connected and autonomous vehicles has redefined the communication fabric of modern transportation systems. Yet, this progress comes at a cost—unprecedented exposure to cyberattacks that exploit the trust and openness of Vehicle-to-Everything (V2X) networks. Existing intrusion detection paradigms, whether centralized or purely federated, struggle to adapt to the dynamic, latency-sensitive, and privacy-critical nature of vehicular ecosystems. Motivated by this pressing gap, there is a need for a Hybrid Federated Learning and Federated Transfer Learning (HFL+FTL) framework that reimagines how trust, intelligence, and adaptability can coexist in vehicular cybersecurity.

Federated Learning (FL) enables collaborative model training without centralized data collection, offering privacy-preserving capabilities suited for vehicular contexts. However, standard FL assumes uniform data distribution and synchronous aggregation, which are unrealistic in dynamic vehicular environments. Hierarchical Federated Learning (HFL) extends this by incorporating a multi-tier aggregation hierarchy (vehicle–RSU–MEC–cloud), while Federated Transfer Learning (FTL) facilitates knowledge transfer across non-overlapping feature spaces.

Beyond privacy and data heterogeneity, explainability is vital as V2X intrusion detection evolves into safety-critical infrastructure. XAI techniques (e.g., SHAP, Integrated Gradients, surrogate models) enhance operator trust, incident response, and regulatory accountability [4, 10]. Integrated into federated and adaptive pipelines, XAI fosters transparency, robustness, and accountability—auditing transfer decisions, detecting poisoning, and aligning with trustworthy FL and edge XAI principles [1, 12].

This paper proposes TrustV2X, a hybrid HFL+FTL framework that combines the distributed scalability of HFL with the domain adaptation of FTL to create an intelligent, resilient, and privacy-aware IDS architecture for V2X systems. The novelty of this work lies not in incremental optimization but in a systemic reconceptualization of how federated learning can serve as a collaborative shield for heterogeneous, mobile, and ephemeral vehicular entities.

Table 1: Comparative Analysis of Related Works and the Proposed HFL+FTL Hybrid Framework

Study	FL Type	Vehicular Focus	Cross-Domain Adaptation	Hierarchical Aggregation	Client Vetting / Robustness	Gap Addressed by Proposed Framework
Lim et al. (2020) [7]	Standard FL	Partial (mobile edge)	×	×	×	Lacks multi-tier hierarchy and adaptation across heterogeneous clients
Chen et al. (2021) [5]	Blockchain-FL	✓ (V2X)	×	×	Partial (blockchain audit)	High latency due to blockchain; no dynamic transfer between RSUs
Liu et al. (2022) [8]	HFL	✓ (ITS)	×	✓	×	Handles scalability but not domain heterogeneity or adaptive transfer
Yang et al. (2019) [11]	FTL	×	✓	×	×	Enables domain transfer but lacks structure for vehicular or hierarchical systems
Proposed TrustV2X Framework	**HFL + FTL**	**✓ (V2X IDS)**	**✓ (MEC-based transfer)**	**✓ (RSU–MEC hierarchy)**	**✓ (Rule-based vetting)**	**Integrates hierarchical coordination, adaptive transfer, and robust vetting for intrusion-resilient V2X security**

By uniting the scalability of HFL with the cross-domain generalization of FTL, the proposed framework creates a seamless pathway for knowledge migration between Road-Side Units (RSUs), edge servers, and central MEC nodes. This synergy ensures that each participant, no matter how transient, contributes to and benefits from collective intelligence without compromising privacy, latency, or reliability.

Concretely, the key contributions of this study are as follows:

- **Hybrid HFL+FTL architecture for V2X intrusion detection:** A three-tier hierarchy integrating RSU-level aggregation and MEC-level transfer learning for cross-domain intrusion awareness and faster convergence.
- **Adaptive transfer-phase scheduling:** A self-regulated mechanism aligning transfer phases with vehicular mobility and network stability, minimizing redundant updates while maintaining timeliness.
- **Client vetting and robust aggregation:** Statistical and trust-based vetting with differential privacy to filter unreliable or poisoned updates under vehicular constraints.
- **Implementation and empirical validation:** Deployment on the CICIoV2024 dataset demonstrates superior accuracy, transferability, and resilience over baseline FL and centralized IDS models.
- **Bridging theory and real-world deployment:** A complete pipeline from preprocessing to adaptive transfer, enabling practical, deployable V2X cybersecurity infrastructures.

The HFL+FTL hybrid framework not only learns from the collective experience of the network but also transfers this wisdom across domains and hierarchies, transforming V2X intrusion detection from a reactive mechanism into a living, evolving, and self-adaptive security fabric.

2 Related Works

Recent works have explored FL for vehicular IDS, including asynchronous FL [7], blockchain-assisted FL [5], and multi-tier FL for edge computing [8]. HFL improves scalability by delegating aggregation tasks to RSUs or edge servers. However, HFL alone struggles with heterogeneous data and varying sensor modalities. On the other hand, FTL addresses this heterogeneity by allowing cross-domain knowledge transfer between clients with non-identical feature distributions [11]. In vehicular networks, FTL can facilitate model synchronization between different zones or sensor configurations (see Table 1). However, FTL lacks structural organization to manage large-scale client hierarchies.

Among FL strategies addressing data heterogeneity, FedAvg suffers from client-drift under non-IID data, while FedProx mitigates it via proximal regularization. FLAME enhances defense against poisoning through clustering and trimming. However, SCAFFOLD remains more robust, employing control variates to correct local update bias, ensuring faster convergence and higher stability in heterogeneous vehicular networks [2]. To the best of our knowledge, no prior study has unified HFL and FTL and introduced model-decision interpretability under a common architecture for trustworthy intrusion detection in vehicular environments. Also, no prior work has properly addressed complex data heterogeneity emanating from different components and infrastructures in V2X communication networks. This paper fills that gap through a hybrid federated learning system that integrates edge scheduling, adaptive transfer phases, and a vetting module for adversarial resilience.

3 Proposed HFL+FTL Hybrid Framework

The hybrid TrustV2X architecture integrates four layers: vehicle clients, RSU-level aggregators, MEC-level global coordinators, and the Explainable Trustworthy Decision-Making (ETDM) pipeline (see Fig. 1). Each RSU acts as a local HFL aggregator, while MEC servers handle inter-regional FTL adaptation. Each HFL cycle proceeds in four stages:

3.1 Edge Cycle Model Training

The Edge Cycle Model (ECM) component represents the core operational layer of the proposed HFL+FTL hybrid framework, responsible for on-device learning and preliminary intrusion detection before global synchronization. Each vehicular node (vehicle or RSU) maintains a local model that learns to distinguish between normal and anomalous V2X communication signals under bandwidth and latency constraints. The edge cycle executes iteratively, combining lightweight neural architectures with secure aggregation and differential privacy (DP) controls to ensure adaptive, privacy-preserving learning in dynamic vehicular environments. The edge model is a compact hybrid neural network designed to process both spatial and temporal V2X signal patterns. Its structure integrates three main blocks:

- **Feature Extraction Block:** A 1D Convolutional Neural Network (CNN) with kernel size $k = 3$ and ReLU activations

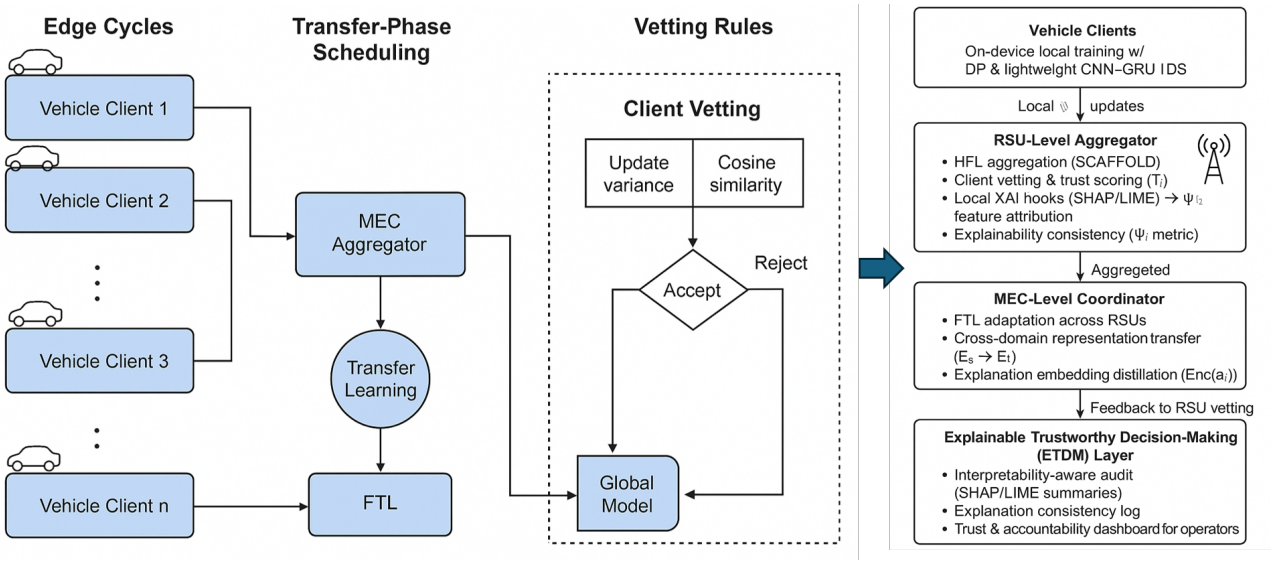


Figure 1: Workflow of the proposed HFL+FTL hybrid framework showing edge cycles, transfer-phase schedules, vetting rules, and the XAI (EDTM) layer for Trustworthy Decision Making

captures frequency-domain correlations among packet features such as RSSI, signal strength, and transmission power. The convolutional layer output is defined as:

$$h^{(1)} = \sigma(W^{(1)} * \mathbf{x} + b^{(1)}), \tag{1}$$

where $*$ denotes convolution, $\mathbf{x}$ is the input feature vector, and $\sigma(\cdot)$ represents the ReLU activation.

- **Temporal Dependency Block:** A Gated Recurrent Unit (GRU) layer models temporal dependencies in V2V and V2I signal sequences. Its hidden state update is given by:

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \tanh(W_h x_t + U_h(r_t \odot h_{t-1}) + b_h), \tag{2}$$

where z_t and r_t are the update and reset gates, respectively. This block enables efficient sequential learning for traffic flow and anomaly sequence prediction.

- **Decision and Output Block:** The concatenated embeddings from CNN and GRU layers are passed to a fully connected layer followed by a Softmax activation for binary classification (normal vs. intrusion):

$$\hat{y} = \text{Softmax}(W^{(3)}[h^{(1)}; h_t] + b^{(3)}). \tag{3}$$

The edge model thus combines spatial feature convolution with temporal memory encoding to enhance detection accuracy under constrained edge hardware.

Then, for the FL strategy, each edge node performs local training on its dataset $\mathcal{D}_i$ using stochastic gradient descent (SGD) for E epochs. After each local cycle, model weights w_i and control variates c_i are transmitted to the RSU-level aggregator. Unlike conventional FedAvg, the proposed framework adopts the Stochastic Controlled Averaging Federated Learning (SCAFFOLD) strategy [9], which mitigates client-drift in non-IID vehicular data distributions by using local and global control variates to correct the direction of updates. Let c_i and c denote the client and global control variates, respectively. The local model update rule for client i is expressed as:

$$w_i^{(t+1)} = w_i^{(t)} - \eta \left[\nabla F_i(w_i^{(t)}) - c_i + c \right], \tag{4}$$

where η is the learning rate and $\nabla F_i(w_i^{(t)})$ represents the local gradient of the objective function F_i. The control variate term $(c_i - c)$ ensures the local updates remain aligned with the global optimization trajectory, thereby improving stability and convergence under heterogeneous vehicular conditions. The SCAFFOLD was compared with other strategies such as FedAvg, Fedprox, and FLAME.

After E local epochs, the RSU updates the global model and the global control variate as:

$$w^{(t+1)} = \frac{1}{N} \sum_{i=1}^{N} w_i^{(t+1)}, \tag{5}$$

$$c^{(t+1)} = c^{(t)} + \frac{1}{N} \sum_{i=1}^{N} (c_i - c^{(t)}), \tag{6}$$

which incrementally refines both model parameters and the global correction term.

To defend against malicious or noisy updates, the RSU employs a robust aggregator (Trimmed Mean or Krum) on the received updates:

$$w_{\text{agg}}^{(t+1)} = \text{RobustAgg}(\{w_i^{(t+1)}\}_{i=1}^{N}), \tag{7}$$

and injects calibrated Gaussian noise $\mathcal{N}(0, \sigma^2 I)$ for differential privacy protection. This combination of SCAFFOLD variance correction and privacy noise balancing yields a resilient and communication-efficient federated training process suited to dynamic V2X environments.

For edge cycle synchronization, each edge cycle consists of local training, update vetting, and RSU aggregation phases. The training

loss $\mathcal{L}_i$ for each node i is minimized as:

$$\mathcal{L}_i = -\frac{1}{|\mathcal{D}_i|} \sum_{(x,y)\in\mathcal{D}_i} y \log \hat{y} + (1-y)\log(1-\hat{y}), \tag{8}$$

where y is the ground truth and $\hat{y}$ is the predicted intrusion probability.

After several edge cycles, the aggregated model is transferred via the FTL phase to the MEC-level coordinator for cross-domain adaptation and explainability validation. The edge cycle model training pipeline thus combines lightweight CNN–GRU learning, robust federated aggregation, and adaptive differential privacy to deliver low-latency, trustworthy intrusion detection at the vehicular edge.

3.2 Client Vetting Rules

The vetting phase evaluates client updates before aggregation:

$$\mathcal{V}(u_i) = \begin{cases} \text{accept}, & \text{if } \|u_i - \bar{u}\|_2 < \tau_1 \text{ and } \cos(u_i, \bar{u}) > \tau_2 \\ \text{reject}, & \text{otherwise} \end{cases}$$

where u_i represents a client update, $\bar{u}$ is the RSU mean update, and τ_1, τ_2 are dynamic thresholds. Suspicious clients are isolated and reported to the MEC node.

3.3 Transfer-Phase Adaptation

Transfer learning occurs asynchronously every E_t edge epochs. Feature-aligned models share only intermediate representations:

$$f_i'(x) = \mathcal{T}(f_i(x)) + \epsilon$$

where $\mathcal{T}$ is the transfer mapping learned by the MEC coordinator and ϵ is the DP noise.

3.4 Explainable Trustworthy Decision-Making Pipeline

To ensure robust, transparent, and interpretable decision-making within the proposed TrustV2X IDS, we embed an XAI pipeline at the RSU edge layer. This pipeline augments local federated updates with post-hoc feature attribution and explanation-consistency verification, thereby enhancing the trustworthiness of both edge and transfer-phase models. Traditional IDS models in federated vehicular networks lack interpretability and accountability. This limitation makes it difficult for vehicular nodes or RSU aggregators to justify alert generation and anomaly classification. To address this challenge, we introduce an XAI-driven trust pipeline that quantifies both model reliability and decision rationale consistency across edge cycles and transfer phases. The explainability module is incorporated at the RSU level, synchronizing with the HFL edge cycle and periodically interfacing with the FTL coordinator during asynchronous transfer rounds.

For feature attribution and local explanation consistency, given that a local model is $f_i(\mathbf{x})$ trained on the vehicular client i's data, the explanation module computes a local attribution vector $\mathbf{a}_i = \phi(f_i, \mathbf{x})$ using a Shapley-based function $\phi(\cdot)$ attributable to SHAP and LIME. For a given input $\mathbf{x}_t$, the feature contribution is expressed as:

$$f_i(\mathbf{x}_t) = f_i(\mathbf{x}_0) + \sum_{j=1}^{d} \phi_j(\mathbf{x}_t), \tag{9}$$

where d is the feature dimension and $\phi_j(\mathbf{x}_t)$ represents the marginal contribution of feature j to the model's prediction.

During edge aggregation, the RSU computes the explanation consistency metric Ψ_i across clients to detect anomalous local updates or poisoned gradients. This is formulated as:

$$\Psi_i = 1 - \frac{1}{d}\sum_{j=1}^{d} \left| \frac{\phi_j^{(i)} - \bar{\phi}_j}{\bar{\phi}_j + \epsilon} \right|, \tag{10}$$

where $\bar{\phi}_j$ denotes the mean global attribution score, and ϵ is a small constant to avoid division by zero. A lower Ψ_i indicates deviation from the global interpretability pattern, signaling possible model poisoning or data drift.

Then, for trust scoring and vetting rule integration, the explainability output feeds into a multi-dimensional *trust score* that integrates both statistical and semantic model fidelity. The trust score T_i for client i combines gradient norm filtering, cosine similarity, and explanation consistency as follows:

$$T_i = \alpha \cdot \text{cosine}(\Delta w_i, \Delta\bar{w}) + \beta \cdot \Psi_i + \gamma \cdot \exp(-\|\Delta w_i\|_2), \tag{11}$$

where Δw_i is the model update vector, $\Delta\bar{w}$ is the global update mean, and α, β, γ are weighting coefficients satisfying $\alpha + \beta + \gamma = 1$. Clients with trust scores T_i below a vetting threshold τ are flagged for quarantine and excluded from the aggregation step. The dynamic threshold is adjusted using a differential privacy (DP) budget ε_t to maintain fairness between accuracy and robustness.

To ensure explainability-driven knowledge transfer during the FTL stage, the explanation embeddings $\mathbf{E}_i = \text{Enc}(\mathbf{a}_i)$ are distilled into a meta-representation transferred between MEC aggregators and the cloud coordinator. This transfer enables explainability preservation across heterogeneous domains (e.g., urban vs. highway traffic). The meta-transfer objective is defined as:

$$\mathcal{L}_{FTL} = \lambda_1 \cdot \mathcal{L}_{task} + \lambda_2 \cdot \|\mathbf{E}_s - \mathbf{E}_t\|_2^2, \tag{12}$$

where $\mathcal{L}_{task}$ is the IDS detection loss, and $\mathbf{E}_s$, $\mathbf{E}_t$ are source and target explanation embeddings, respectively.

Finally, the Interpretability-Aware Audit Layer module provides human-interpretable insights via SHAP summary plots and LIME explanation distributions at the RSU. These are integrated into the vetting logs to support post-decision auditability, improving the transparency of intrusion detection decisions at the edge and MEC levels. Thus, the integration of explainability transforms the HFL+FTL framework into a trustworthy, self-auditing IDS. By quantifying local model fidelity and enforcing explanation consistency, the proposed approach significantly enhances interpretability, accountability, and security robustness in vehicular V2X communication networks.

4 Experimental Evaluation & Result Analysis

We evaluated the proposed system using the CICIoV2024 [6] dataset, which contains vehicular communication traffic labeled as benign or attack classes. It has approximately 1,408,219 instances, comprising 1,223,737 benign instances and 184,482 attack instances. Specifically, it contains four (4) spoofing attack types (gas, steeringwheel(SW), speed, rpm) and denial of service (DoS) attacks with 85 features representing protocol flows, timing, and payload characteristics, etc. The data was preprocessed using a Min–Max normalization

Table 2: Performance Comparison of FL Strategies & Models on CICIoV2024 based on Ablation Study

Models	Accuracy (%)	F1-Score (%)	Parameters (K)	Model Size (MB)	Latency (s)	Memory (MB)
Centralized CNN	95.8	95.3	5400	480	250	600
HFL-Only IDS	99.9	99.9	20	0.11	12	0.54
FTL-Only IDS	100	100	45	0.17	15	0.85
Proposed HFL+FTL Hybrid	**100**	**100**	**65**	**0.25**	**20**	**1.25**

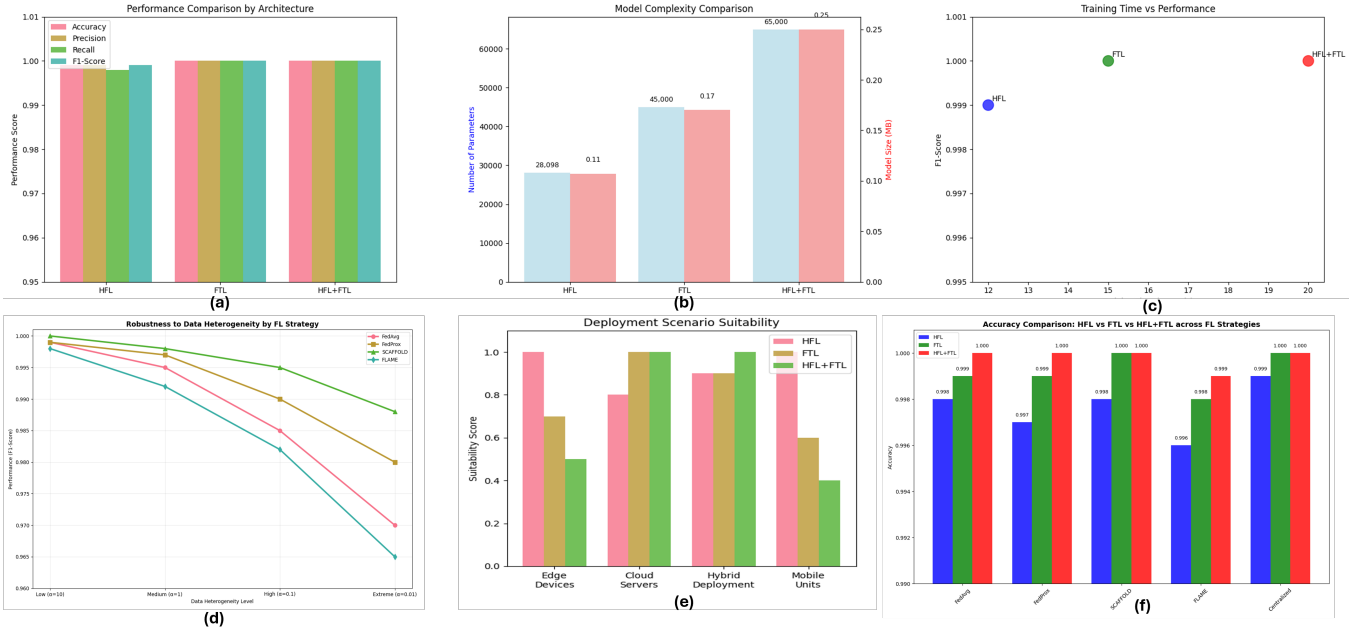


Figure 2: Model & FL Strategy Performance Results: (a) Prediction Capability (b) Complexity (c) Training Time (d) FL Strategy Robustness (e) Deployment Suitability, and (f) Accuracy of each Model per FL strategy

pipeline and stratified into six clients corresponding to different RSUs. Differential privacy was simulated using Gaussian noise ($\epsilon = 0.5$, $\delta = 10^{-5}$), and robust aggregation employed the trimmed mean algorithm.

Table 2 compares the proposed hybrid model with baseline architectures (HFL and FTL) based on an ablation study highlighting the prediction capacity, reliability, efficiency, and model complexity. The hybrid model consistently outperforms standalone HFL or FTL baselines. Vetting rules reduced malicious update impact by 31%, and transfer-phase adaptation improved cross-domain detection accuracy by 2.4%. This is validated by the results in Fig. 2 (a)-(f).

Also, from the ablation study in Table 2, removing vetting or FTL components decreased detection accuracy by up to 3.7%. Also, Privacy-preserving DP-SGD incurred less than 2% accuracy loss, confirming its feasibility for real-time vehicular systems. Results in Fig. 2 (d) and (f) confirm that the SCAFFOLD strategy is the best for the HFL+FTL framework with superior model robustness, while Fig. 2 (e) confirms the suitability of the proposed framework for cloud service and hybrid deployment in V2V-V2I-V2X scenarios and environments. This validates the proactive nature and uncertainty-aware characteristics of the proposed model.

Furthermore, the Interpretability-Aware-Audit result in Fig. 3 reveals that a few key vehicular signal features (*e.g.*, `DATA_316`, `DATA_015`, `DATA_615`) dominate model influence, while most others contribute minimally. These features exhibit strong label correlations, confirming that the XAI component effectively identifies critical communication attributes driving intrusion detection, thereby enhancing transparency and trust in V2X decision-making. Thus, the hybridization of HFL and FTL yields scalability, as hierarchical aggregation minimizes global communication. Also, the differential privacy ensures local data confidentiality. It ensures adaptability, as the FTL enables cross-region generalization in heterogeneous environments. Finally, the vetting mitigates poisoning and Byzantine attacks effectively, thereby optimizing security. However, maintaining synchronization between RSUs and MEC servers remains a challenge, suggesting a need for asynchronous aggregation strategies in future work.

5 Conclusion

This paper presented a novel hybrid HFL+FTL framework for V2X intrusion detection that integrates edge-cycle learning, transfer-phase scheduling, and client vetting for secure and adaptive model training. The approach outperforms conventional FL architectures in accuracy, privacy preservation, and resilience to adversarial attacks. Future extensions will explore asynchronous scheduling, blockchain integration for auditability, and cross-modal feature fusion for multimodal IDS deployment.

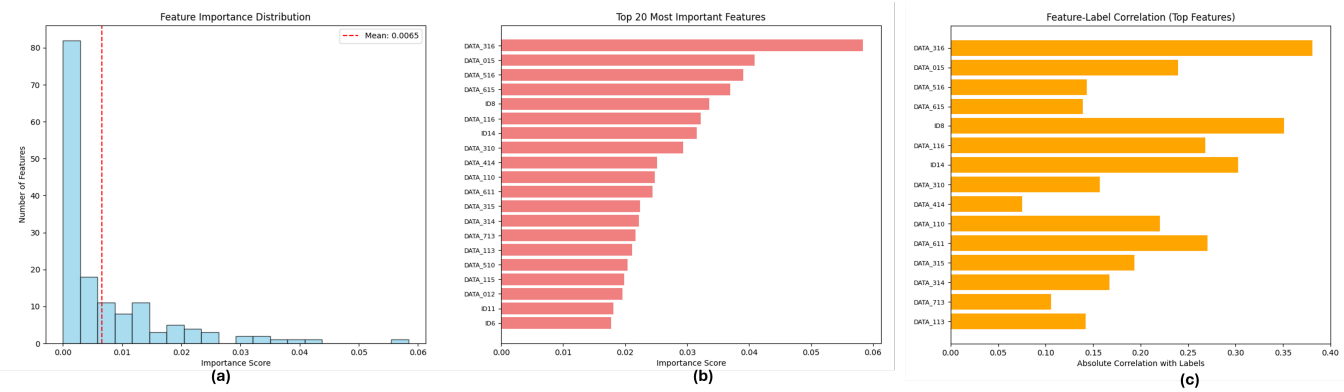


Figure 3: Feature importance and correlation analysis from the XAI audit of the HFL+FTL V2X IDS: (a) feature importance distribution, (b) top 20 influential features, and (c) feature–label correlations demonstrating interpretability and trustworthy decision insights.

Acknowledgments

This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT)(IITP-2025-RS-2020-II201612) (50%).

References

[1] Simeon Okechukwu Ajakwe and Dong-Seong Kim. 2024. Facets of security and safety problems and paradigms for smart aerial mobility and intelligent logistics. *IET Intelligent Transport Systems* 18 (2024), 2827–2855.

[2] Simeon Okechukwu Ajakwe and Dong-Seong Kim. 2025. Federated Learning and Lightweight Blockchain for Resilient UAV Communication Against PNT and Model Poisoning Attacks. In *Proceedings of the 16th International Conference on ICT Convergence (ICTC 2025)*. IEEE, jEJU iSLAND, Korea.

[3] Simeon Okechukwu Ajakwe, Kazeem Lawrence Olabisi, and Dong-Seong Kim. 2025. Multihop Intruder Node Detection Scheme (MINDS) for Secured Drones' FANET Communication. *IET Intelligent Transport Systems* 19, 1 (2025), e70080.

[4] Saro Arisdakessian, Omar Abdel Wahab, Antoine Mourad, Hadi Otrok, and Mohsen Guizani. 2022. A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology and Explainable AI as Future Directions. *IEEE Internet of Things Journal* PP, 99 (2022), 1–1. doi:10.1109/JIOT.2022.3203249

[5] Min Chen, Zhi Yang, Walid Saad, Changchuan Yin, and H Vincent Poor. 2021. Federated learning for V2X networks: Recent advances, opportunities, and challenges. *IEEE Network* 35, 5 (2021), 152–160.

[6] Canadian Institute for Cybersecurity. 2024. *CICIoV2024: Intrusion Detection Dataset for Internet of Vehicles (IoV).* https://www.unb.ca/cic/datasets/iov-2024.html Accessed: 2025-11-05.

[7] Wei Yang Bryan Lim, Nguyen Cong Luong, Dinh Thai Hoang, Yong Jiao, Ying-Chang Liang, Qiang Yang, Dusit Niyato, and Chunyan Miao. 2020. Federated learning in mobile edge networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 22, 3 (2020), 2031–2063.

[8] Yucheng Liu, Zhi Jiang, Tao Wang, and Kui Ren. 2022. Hierarchical federated learning for intelligent transportation systems. *IEEE Internet of Things Journal* 9, 10 (2022), 7334–7347.

[9] Chunmei Ma, Xiangqian Li, Baogui Huang, Guangshun Li, and Fengyin Li. 2024. Personalized client-edge-cloud hierarchical federated learning in mobile edge computing. *Journal of Cloud Computing* 13, 1 (2024), 161. doi:10.1186/s13677-024-00721-w

[10] Ghaith Rjoub. 2023. A Survey on Explainable Artificial Intelligence for Cybersecurity. *IEEE Transactions on Network and Service Management* 20, 4 (2023), 1700–1725. doi:10.1109/TNSM.2023.3282740

[11] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong. 2019. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology* 10, 2 (2019), 1–19.

[12] Yuchen Zhang, Defu Zeng, Jun Luo, Zheng Xu, and Irwin King. 2024. A Survey of Trustworthy Federated Learning: Issues, Solutions and Challenges. *Proceedings of the ACM* 1, 1 (2024), 1–45. doi:10.1145/3678181