E-ISSN: 111 – 2716 P-ISSN: 3026 – 8214
MPRI-JAAER | INTERNATIONAL JOURNAL OF APPLIED & ADVANCED ENGINEERING RES.
VOL. 10 NO. 5 OCTOBER, 2025

# FEDERATED MACHINE LEARNING-BASED CYBERSECURITY FRAMEWORK FOR AUTONOMOUS AND CONNECTED VEHICLES: PRIVACY-PRESERVING REAL-TIME INTRUSION DETECTION AND ADAPTIVE THREAT MITIGATION IN V2X COMMUNICATIONS

***MICHAEL OGHALE IGHOFIOMONI; **YUSUF AKINKUNMI BADRUDEEN; ***ABIMBOLA OLUDAYO OJENIKE; ****OLAYEMI ELIJAH SAMSON; *****SAMUEL OLAOLUWA ABIOYE; ******CONFIDENCE ADIMCHI CHINONYEREM; & *******OLUSEGUN OLAYINKA SOFOWOKE**

*Southern Delta University, Ozoro, Nigeria, Department of Computer Engineering and Systems Engineering. **Airforce Institute of Technology, Kaduna, Nigeria, Department of Cyber Security. ***Olabims Integrated Services Ltd, Ajah, Lagos. ****University of Ilorin, Nigeria, Department of Civil Engineering. *****University of Ilorin, Nigeria, Department of Civil Engineering. ******Abia State Polytechnic, Nigeria. *******Federal University of agriculture abeokuta Department of statistics

**DOI:** https://doi.org/10.70382/mejaaer.v10i5.044

## Abstract

The increasing interconnectivity of autonomous and connected vehicles (ACVs) has intensified cybersecurity challenges within Vehicle-to-Everything (V2X) communications. This study presents a Federated XGBoost-Based Cybersecurity Framework designed for privacy-preserving, real-time intrusion detection and adaptive threat mitigation. Using the VeReMi Extended Dataset, the framework [redacted] collaboratively trains distributed models across multiple vehicular nodes without sharing raw data, thereby enhancing data privacy and scalability. Twelve major cyberattack types including Sybil, Wormhole, Flooding, GPS Spoofing, and Denial of Service (DoS) were analyzed following extensive

**Keywords:** Learning-Based Cybersecurity Framework, Autonomous Connected Vehicles: Privacy-Preserving.

EDITOR-IN-CHIEF
**Prof. Saeid Eslamian [IRAN]**

preprocessing, feature selection, and class balancing. The proposed federated model achieved 86.44% accuracy, 87.03% precision, 86.44% recall, and an F1-score of 85.19%, demonstrating strong multiclass detection performance. High precision was observed for Fabrication (F1 = 0.98) and Sybil (F1 = 0.96) attacks, while routing-based attacks such as Sinkhole and Blackhole showed moderate detection due to behavioural similarities. Compared with local client models, the federated approach achieved improved generalization and privacy preservation across heterogeneous vehicular datasets. These findings confirm that federated gradient boosting offers an efficient, scalable, and privacy-aware solution for vehicular intrusion detection. Future work will integrate hybrid deep–boosted architectures and blockchain-based secure aggregation to enhance zero-day attack detection and model integrity in intelligent transportation systems.

## Introduction

Autonomous and connected vehicles are revolutionizing contemporary transportation by Eze et al. (2025) integrating cutting-edge sensing, control, and Vehicle-to-Everything communications to enhance safety, (Yusuf et al., 2023) efficiency, and traffic management. With V2X, including Vehicle-to-Vehicle (, Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) communication (Ben Khadra, 2023), Ji et al. (2024) conducted a survey on cooperative vehicle-infrastructure systems for autonomous driving, according to Ji et al. (2024) vehicles share critical information like position, velocity, and hazard alerts to facilitate cooperative driving and enhance road safety. Though these characteristics enhance the sensing and decision-making ability of vehicles, they also expand the system's attack surface (Rahimi et al., 2025), making vehicular networks vulnerable to cyber attacks like message spoofing, denial-of-service, Sybil attacks, and remote-control system takeover (Venkatasamy et al., 2024). These vulnerabilities indicate that cybersecurity is not a plug-in but a must for deploying intelligent transportation systems in a secure manner.

The job of protecting V2X environments is also complicated by a number of critical factors. One, intrusion detection must be performed either in real time or nearly real time since the latency involved in detecting or reacting to threats can have disastrous outcomes (Nandy et al 2024). Two, the volume of data collected by vehicles typically tends to be sensitive data, like data related to driver habits, routes, and locations, and thus presents enormous privacy concerns in case centralized data collection is utilized. Third, computing and communication resources of roadside and vehicles' units are generally restricted, and

hence resource-intensive detection models are not feasible. Second, vehicular settings are inherently heterogeneous and hence data distributions differ from region to region, time to time, and from manufacturer to manufacturer, and it is difficult to deploy centralized or fixed security solutions. Finally, the adversaries can utilize these weaknesses intentionally, poisoning learning-based detectors or evading defences using adaptive attack methods (Chong et al., 2025). Machine learning has also been shown to be a powerful method of intrusion detection in automotive networks since it has the capability of detecting sophisticated (Samson & Iseal, 2025), high-dimensional attack patterns that would be challenging to do with conventional rule-based methods. Legacy centralized machine learning systems carry the limitation of raw vehicle data having to be aggregated at the point of contact, hence creating more privacy threats and subjecting huge communication burdens. (He et al., 2025) Federated learning (FL) (Zhang, et al 2024) overcomes these limitations via the provision of distributed clients like roadside units or vehicles to collaboratively train models without sharing data. Model update only is transferred and aggregated into a global model, (Myakala,et al 2024) minimizing exposure to privacy as well as communication expenditure but allowing sharing of information among multiple participants (Sebastian et al., 2023). This paradigm is particularly well-suited to V2X applications where scalability and privacy protection are critical. Promising as it is, federated learning for V2X cybersecurity does come with some challenges yet to be solved. Gradient or weight updates could still leak sensitive information unless supplemented by mechanisms such as differential privacy or secure aggregation, though the latter could sacrifice accuracy or introduce latency. In addition, federated systems are susceptible to poisoning attacks where adversaries provide poisoned updates that contaminate the global model (Mao et al., 2021). The natively non-identically distributed and non-IID vehicular data makes it harder to train and converge models, while the dynamic mobility and intermittent connectivity of vehicles necessitate communication-efficient and communication-light protocols. Moreover, intrusion detection is not enough without mitigation. Upon sensing an intrusion, infrastructure and vehicles need to react with adaptive countermeasures like isolating the malicious nodes, filtering out the infected messages, or dynamically updating the trust scores. Static policies are typically not sufficient against adaptive cyber attacks, and this requires adaptive, feedback-based mitigation techniques to guarantee resilience in real-world deployments (Çetinkaya et al., 2025).

**PROBLEM STATEMENT**

The explosive growth of interconnected and autonomous vehicles brought new opportunities for intelligent transportation, but also high-end cybersecurity threats.



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

Vehicle-to-everything communication allows real-time exchange among vehicles, roadside units, and infrastructure, but is hugely exposed to fake attacks like data tampering, spoofing, and denial-of-service. Conventional centralized intrusion detection systems are not feasible in this case, as they involve transmitting raw sensitive data to a central server, which poses privacy threats and can even hinder real-time decision-making. Furthermore, the dynamic and heterogeneous nature of vehicular communication networks renders static detection techniques ineffective in adapting to changing threats. These issues underscore the importance of having a privacy-assuring, adaptive, and decentralized security system that is capable of identifying and repelling cyber attacks successfully without divulging confidential driving or communication information.

**OBJECTIVES OF THE STUDY**

- The overall goal of this research is to develop and analyze a privacy-guaranteeing cybersecurity framework for autonomous and networked vehicles that allows for intrusion detection and adaptive threat mitigation in vehicle-to-everything communication systems. The detailed objectives are to:
- Design a decentralized intrusion detection method with reduced use of centralized data gathering and safeguard sensitive vehicular information.
- Imbue state-of-the-art collaborative learning mechanisms to support improved detection accuracy across various vehicular communication environments.
- Integrate adaptive threat mitigation capabilities that enable the system to dynamically react to new and emerging cyber threats in real-time.
- Compare the performance of the proposed framework with state-of-the-art centralized detection systems utilizing benchmark intrusion detection data sets and validate its effectiveness.
- Illustrate how the framework can ensure high security performance as well as privacy protection for large vehicular networks.

**RELATED SURVEY**

In recent years, federated learning has become a key paradigm to enable collaborative model training across distributed devices without revealing raw data. It has been particularly employed by researchers in networked system intrusion detection and cybersecurity. For example, a comprehensive survey by Zhou et al. (2025) describes the growing use of federated learning in intrusion detection and cites its data privacy advantage while supporting collective intelligence (Zhou et al. 2025). In line with that argument line, Zhang et al. (2025) survey privacy-preserving collaborative learning

techniques in federated environments and remark on difficulties like communication overhead, client heterogeneity, and adversarial attack robustness (Zhang et al. 2025).

Federated learning is used in the context of IoT to develop intrusion detection systems with the protection of users' information. Shayan et al. (2024) introduce a near-real-time intrusion detection for IoT using a hybrid federated approach with local and global learning and resource-constrained device privacy enforcement (Shayan et al. 2024). Similarly, Chen, Chen, and Zhao (2024) put forward a differential privacy-boosted sparsified federated learning solution to reduce the cost of communication and improve the privacy–utility trade-off (Chen et al. 2024). For applications in vehicles, Wang et al. (2024) propose a federated learning–based in-vehicle communication bus intrusion detection system, which proves the possibility of local model training and aggregation of parameters for anomaly detection with less data exposure (Wang et al. 2024).

Another research direction is to combine federated learning and privacy-preserving mechanisms. For example, Ma et al. (2021) introduce a multi-key homomorphic encryption scheme (xMK-CKKS) to encrypt updates of parameters under federated training homomorphically, thereby circumventing leakage even when model weights are communicated (Ma et al. 2021). Briggs, Fan, and Andras (2020) also introduce a survey of privacy-preserving federated learning methodologies to the Internet-of-Things, outlining trade-offs between communication efficiency, differential privacy, and cryptography (Briggs et al. 2020). Recently, ElZemity and Arief (2024) present an exhaustive account of federated learning privacy attacks and defence techniques and list inference attacks, poisoning, and eavesdropping as the most significant risks and classify defence strategies according to them (ElZemity & Arief 2024).

Adversarial robustness is another area of focus. Bonawitz et al. (2017) recommended secret sharing with double-masking to protect federated aggregation against dropouts or colluding players (Bonawitz et al. 2017). Singh et al. (2023) apply layered trust models, which reduce the weightage of malicious clients' gradient contributions in intrusion detection and enhance adversarial updates' resistance. At the same time, Xu et al. (2025) introduce adaptive model update filtering according to gradient similarity measures as a countermeasure to the poisoned contributions effect.

For such vehicle networks, vehicle communications have recently witnessed attempts at deploying federated learning for the purpose of securing communication. Lee and Kim (2023) design a certificateless signature scheme for federated vehicle-to-vehicle messaging in a bid to mitigate computation overhead while maintaining authenticity. Yilmaz et al. (2024) integrate federated learning with blockchain to offer tamper-resistant audit logs for vehicular network model updates for improved accountability and trust. Patel et al. (2025) also utilize a federated meta-learning strategy where each vehicle fine-



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

tunes a global intrusion model to the local traffic pattern and thus enhances local detection accuracy under non-independent data distributions. While the volume of work is increasing, if federated learning is implemented on autonomous and vehicle-to-everything connected automobile systems, there remain gaps. Most works deal with static attack models, and they scarcely utilize adaptive mitigation policies that dynamically update response techniques in real-time. Furthermore, few works optimize all three of privacy, latency, and robustness simultaneously under constraints of vehicular computing settings. These gaps give rise to the necessity for a privacy-safeguarding, standardized federated learning design for intrusion detection and adaptive threat blocking in vehicle-to-everything communications use cases.

**Federated Machine Learning**

Federated machine learning is a distributed learning paradigm where multiple independent clients jointly learn an aggregated global model without sharing inter-client raw training data. Rather than aggregating local records into a single repository, users perform local model updates and send only local updates (e.g., model weights or gradients) to an aggregator for secure aggregation; this architecture reduces exposure of private information but facilitates collective model improvement (Konečný et al., 2016; Rothchild et al., 2020).

Privacy protection is the primary motivator of federated learning. Federated schemes minimize the attack surface for centralised data breaches because they don't send raw data, but no matter how hard one tries, they can't eliminate privacy risk since model updates can be information-leaking. A number of efforts have hence merged federated learning with rigorous privacy protection, i.e., differentially private update perturbation and secure aggregation protocols; the mechanisms are designed to avoid recovery of training instances but maintain utility of global model (Mothukuri et al., 2021; Acar et al., 2018). Experimental evidence indicates that cryptographic protection or noise addition entails privacy assurance-model performance trade-offs requiring careful unwinding for successful deployments.

The second primary research direction is to handle statistical heterogeneity: the clients in federated systems typically have non-independently and non-identically distributed data, deterring convergence and lowering the generalized accuracy of one global model. Scholars have introduced personalization and clustering methods so that the federated system is able to provide globally shared knowledge while adapting models to client-specific patterns of data. Structured personalization, client clustering, and subnetwork selection are all valid solutions to address the non-IID problem, and such techniques are

experimentally demonstrated to significantly enhance per-client performance without compromising cooperation (Vahidian et al., 2021; Sáez-de-Cámara et al., 2023).

Communication efficiency is another significant area of current research because networks with numerous clients (or bandwidth-limited clients) cannot always communicate full model updates. Sparse/quantized communication, update sketching, and compression minimize downlink and uplink loads; for example, sketching algorithms enable lossy gradient compression at no cost to efficient mergeability of updates at the aggregator for good scaling over large federations (Rothchild et al., 2020). Periodic aggregation, hierarchical aggregation (edge/cluster aggregators), and client subsampling have further been suggested in order to minimize communication rounds as well as latency in production rollouts.

Stable federated systems need robustness and immunity to malicious players. Since clients may be compromised or become adversaries, aggregation techniques and outlier detection procedures have been made Byzantine-resistant and resilient to poisoning attacks. A series of work investigates robust aggregation rules, gradient-level anomalies, and trust-based client contribution reweighting; jointly, these defences weaken the effect of poisoned updates and enhance the stability of the global model (Mothukuri et al., 2021; Sun et al., 2021).

Cryptographic and secure computation methods constitute an orthogonal research axis. Homomorphic encryption, secure multiparty computation, and order-preserving encryption have been proposed as means of performing aggregation and some computation on encrypted updates with even less risk of leakage. Cryptographic methods enhance confidentiality protection but will generally add computational and communication overhead; therefore, more recent proposals venture into hybrid architectures that use cryptography judiciously (on sensitive parameters or in cross-silo cases) to find security-efficiency balance (Acar et al., 2018; Wibawa et al., 2022).

Lastly, federated learning is now used to solve real-world security issues and Internet of Things application, such as networked device intrusion detection and anomaly detection. Experiments prove that federated intrusion detection can be as precise as centralized baselines without compromising local data privacy, as system designers at the same time address heterogeneity, refresh privacy, and adversarial robustness (Belarbi et al., 2023; Harahsheh et al., 2024). New architectures typically blend federated learning with edge computing, blockchain-based tamper-evident model update logging, and adaptive mitigating modules that transform the detection output into context-adaptive responses at the edge.

Cybersecurity architectures for autonomous and connected vehicles Autonomous and connected vehicles are highly advanced cyber-physical systems whose digital and physical

safety and performance are dependent on sensing, control, software stacks, over-the-air updates, and wide-area communication with infrastructure and other road participants. A cybersecurity architecture for these vehicles thus includes policies, lifecycle risk management, technical controls (authentication, confidentiality, integrity), intrusion detection, secure update mechanisms, and run-time mitigation strategies aimed at safeguarding digital as well as physical safety. The requirement for a well-delineated framework stems from the fact that attacks on vehicle software or communications networks have the potential to lead to direct physical damage or serious privacy invasion (SAE International, 2016; NHTSA, 2016). Threat analysis against autonomous vehicle systems reveals remote exploitation, sensor spoofing, message tampering, denial-of-service, supply-chain compromise, and malicious software update as major threats. Durlik (2024) analyzed the existing attack surface and found that automotive autonomy raises the potential attack surface varying from telematics units to machine-learning perception modules demanding defence-in-depth architectures integrating prevention, detection, and safe-fail responses. Campos (2024) and Bouchouia (2023) also view the function of misbehaviour and anomaly detection as necessary additions to cryptography defence since some attacks (e.g., well-formed but successfully forged messages) evade strict authentication and must be detected through behavioural inspection. Vehicle cybersecurity architecture design has been led by industry and researchers according to standards and guideline regulations. SAE J3061 introduces a lifecycle-focused process for discovering and countering vehicle cybersecurity threats and has been taken up broadly as a practice standard by original equipment manufacturers and suppliers. Government policy, like the U.S. National Highway Traffic Safety Administration's best-practice on cybersecurity, promotes threat-analysis-driven secure design, coordinated vulnerability disclosure, and secure software update practices—principles now fundamental ingredients in many proposed frameworks (SAE International, 2016; NHTSA, 2016). These guidelines emphasize that development activities, testing, and governance follow technical approaches to be effective. Vehicle network intrusion detection systems have evolved into two complimentary categories: in-vehicle network intrusion detection and network-level misbehaviour/anomaly detection. Deep learning and machine learning-based identification of in-vehicle CAN bus anomalies and message injection have been investigated, both of which can be very effective in identifying signal anomalies and message injection if trained on appropriately representative data, but systems do require good feature engineering and features to control false alarms for safety-critical systems (Luo, 2023). At network and cooperative level, detection mechanisms of misbehavior verify timing, plausibility, and patterns of mobility to detect deviant participants or impinging messages; Boualouache et al. (2022) provide a very exhaustive review of those



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

methods and address open problems in reproducibility and large-scale deployment. Those modules of detection belong to the main building blocks of cybersecurity architectures due to the fact that cryptographic approaches will never be able to detect all types of attacks. Lightweight authentication and secure communication are of special research value for vehicular systems due to the need for fast, low-latency message authentication with little computational overhead for cars. Certificate-less and certificateless batch-verifiable aggregate signature schemes have been introduced aiming at minimizing verification overhead without compromising authentication and privacy guarantees; Bouakkaz et al. (2020) and subsequent work show batch-verifiable certificateless signatures optimized for vehicle-to-vehicle communication. Efficient aggregate or batch schemes are particularly attractive for high-density traffic or platooning scenarios were verifying many messages quickly is essential.

The development of cyber safety threats and increasing demand for focused privacy solutions have significantly expanded research into FL applications. While traditional centralized machine learning methods remain strong, they show critical restrictions such as data leakage, narrow communication spots and exposure to individual points of failure. These disadvantages are particularly important in IoT ecosystems, where a huge number of connected devices work over sensitive data protection.

The challenge of learning from non-IID data across heterogeneous clients has led to the development of multi-objective and multi-task FL strategies, with studies showing improved accuracy and fairness in real-world scenarios (Arafeh et al., 2025). In parallel, efforts to integrate FL within distributed cloud computing infrastructures have leveraged SMPC, trusted execution environments, and differential privacy to provide robust and privacy-preserving analytics across nodes (Mccall, 2025).

Personalization in FL has emerged as a key area, enabling the adaptation of models to individual clients while defending against advanced threats. Defense mechanisms based on gradient similarity and layered trust policies have shown improved robustness in countering stealthy backdoor attacks, without compromising collaborative learning Durlik, I. (2024). In dynamic and containerized environments, AI-powered adaptive security meshes have been proposed as complementary to FL, improving threat detection and resilience Boualouache, et al (2022).

Further developments in secure computation include efficient delegable order-revealing encryption schemes that support multi-user range queries over encrypted data an essential capability in federated analytics frameworks Grover, J., et al. (2022. To enhance trust and auditability, blockchain-integrated FL has also gained attention, enabling immutable logs and secure collaboration in decentralized learning systems Bouakkaz, et al (2020). Within smart cities, FL frameworks augmented with lightweight encryption and



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

privacy-preserving mechanisms have been proposed to secure large-scale IoT infrastructures Timofte et al. (2025).

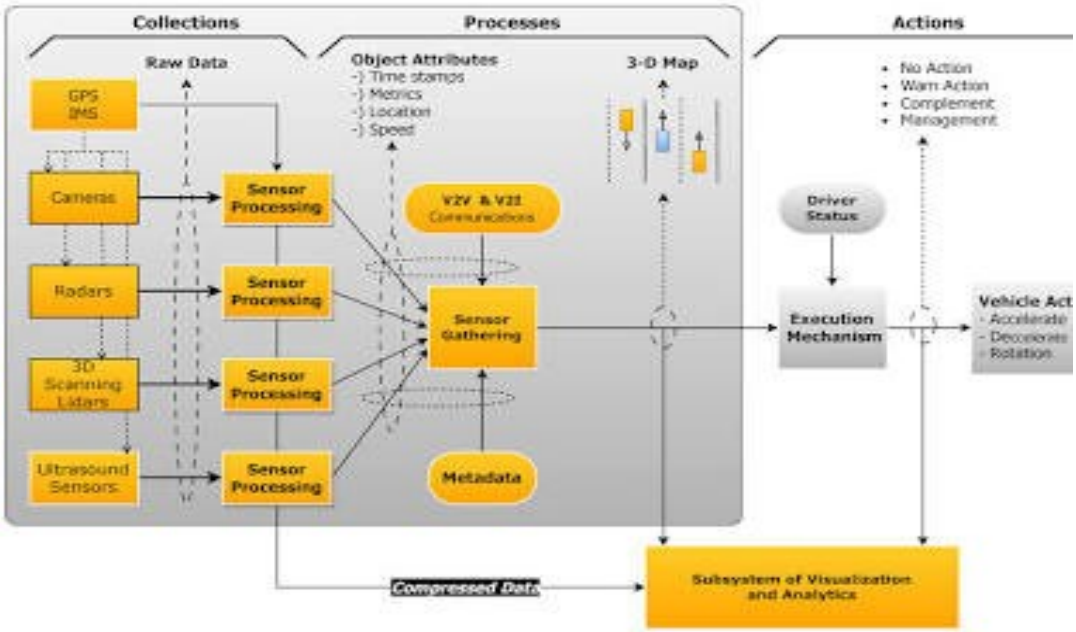



**Figure 1: IoT infrastructures**

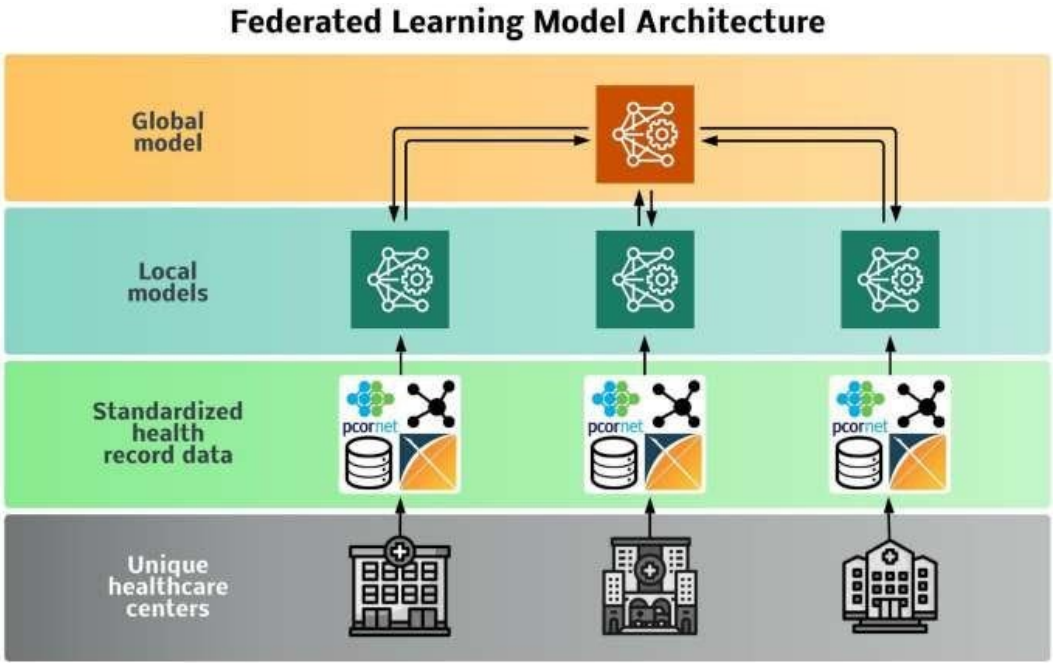



**Figure 2: Cloud Hacks (2024) federated learning model Architecture**

**Dataset Preparation and Feature Engineering**

This study employed the VEREMI Extended Dataset, a widely used benchmark for evaluating intrusion detection systems in connected and autonomous vehicles. The dataset was originally developed by the Hacking and Countermeasure Research Lab (HCRL) at Korea University and later extended to include additional vehicular mobility traces and communication events for Vehicular Ad hoc Networks (VANETs) (Veremi, 2021). The dataset captures Controller Area Network and Vehicle-to-Everything (V2X) communication traffic, representing both normal driving scenarios and multiple classes of cyberattacks targeting vehicular communication layers. The raw dataset comprised approximately 3.19 million samples and 30 features that described physical and network states, including position, speed, acceleration, and heading.

**Feature Selection and Preprocessing**

From the raw data, 24 numerical features were selected, focusing on physical and kinematic attributes relevant to cyberattack detection. These include positional coordinates (posx, posy, posz), speed components (spdx, spdy, spdz), acceleration vectors (aclx, acly, aclz), and heading directions (hedx, hedy, hedz), along with their normalized counterparts. These features collectively represent vehicular motion and communication patterns that can be disrupted or spoofed by adversarial attacks (Hussain et al., 2020). Feature scaling was performed using min–max normalization to rescale all features within the [0,1] range, ensuring model stability and avoiding magnitude bias during gradient-based learning.

**Attack Classes and Data Balancing**

The dataset initially contained 20 labeled attack classes. However, only attacks directly related to cybersecurity threats were retained to align with the research objective of privacy-preserving intrusion detection. The final retained categories include: Normal, Sybil, Wormhole, Replay, Blackhole, Flooding, Eclipse, GPS Spoofing, Jamming, Denial of Service (DoS), Sinkhole, and Fabrication.

Other classes, such as Impersonation, Bogus Information, Selective Forwarding, Resource Exhaustion, and Location Disclosure, were excluded because they either contributed to model overfitting or overlapped semantically with stronger, better-defined attack types. After filtering, the dataset contained approximately 2.54 million attack-related records.

To mitigate data imbalance, particularly the dominance of "Normal" samples, a conservative under sampling strategy was applied. The number of "Normal" samples was limited to approximately twice that of the largest minority attack class. This approach



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

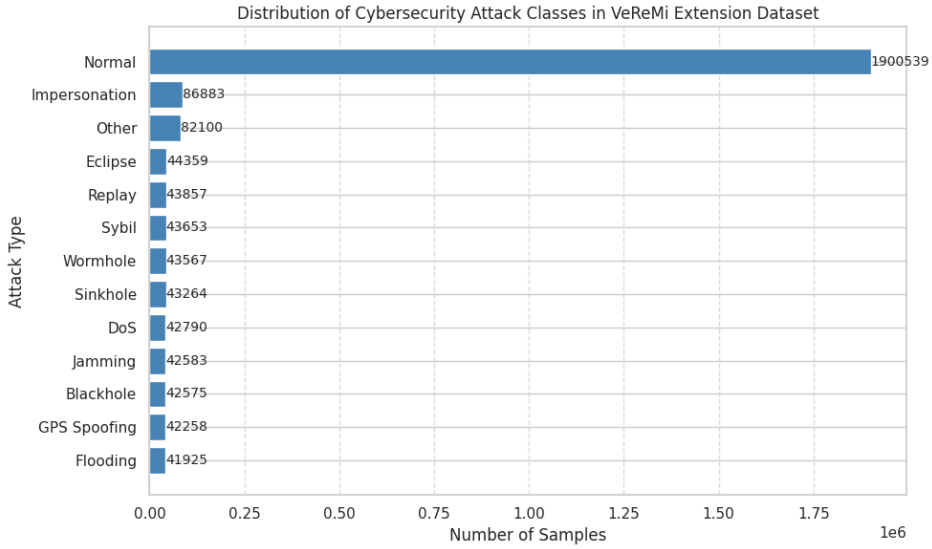
maintained the representativeness of normal driving while ensuring balanced learning across attack categories (Zambudio Martínez et al., 2025).

**Federated Client Partitioning**

The balanced dataset was divided among five simulated clients, representing distributed vehicular nodes or infrastructure units in a federated learning environment. The train_test_split function with stratification was used to preserve class proportions within each client's local dataset. Each client thus contained roughly 140,000 - 150,000 samples, ensuring exposure to all attack types without data leakage across clients. This federated partitioning strategy reflects a realistic scenario in which vehicular agents independently train local models using private data before participating in global aggregation.

**Data Visualization and Analysis**

To visualize the distribution of attacks, a bar chart was generated showing the frequency of each class. The chart revealed that "Normal" data significantly outnumbered other classes, followed by Fabrication and Sybil attacks, while categories such as Flooding, Replay, and Sinkhole had fewer instances. This visualization confirmed the necessity of normalization and under sampling procedures, as they effectively reduced skewness and improved data uniformity before training. Figure 3.1 shows the distribution of cybersecurity attack classes in the VeReMi extension dataset.




**Data Preprocessing**

Prior to model training, extensive preprocessing was conducted to ensure data quality and balanced representation across classes. First, categorical class labels were encoded

into integer indices to facilitate compatibility with machine learning algorithms (Karhana et al., 2025). During exploratory analysis, several attack types, such as Impersonation, Message Suppression, Bogus Information, Resource Exhaustion, and Location Disclosure, were identified as underperforming or fault-related categories, often characterized by extremely low recall and unstable contribution to classifier performance. These classes were excluded from further analysis, consistent with practices in intrusion detection research where rare and noisy categories can bias learning and evaluation (Sangapu et al., 2023). Classes with very low detection reliability and poor separability in earlier experiments, namely Impersonation, Other, Fabrication, Selective Forwarding, Message Suppression, Bogus Information, Resource Exhaustion, and Location Disclosure, were dropped to prevent model dilution.

The resulting dataset retained twelve classes: Normal, Sybil, Wormhole, Replay, Blackhole, Flooding, Eclipse, GPS Spoofing, Jamming, DoS, Sinkhole, and Fabrication. Table 3.1 shows the Taxonomy of Considered Cybersecurity Attacks in Vehicular Networks.

To address class imbalance, we adopted a conservative under-sampling strategy. The Normal class originally accounted for a disproportionate share of the dataset (over 1.2 million samples). To mitigate bias toward this majority class, the number of Normal samples was reduced to twice the size of the largest minority class (approximately 104k samples). This approach preserved sufficient diversity in normal driving patterns while preventing overfitting to benign traffic, an issue highlighted in prior work on intrusion detection in vehicular networks (Zambudio Martínez et al., 2025).

Following class refinement, the dataset was partitioned into 80% training and 20% testing sets using stratified sampling to maintain class proportions. To simulate federated learning, the training set was further divided into five clients of approximately equal size, each preserving the multiclass distribution. These steps ensured a balanced and computationally efficient dataset that improved learning stability while maintaining representativeness of real-world cyberattack patterns.

**Table 1. Taxonomy of Considered Cybersecurity Attacks in Vehicular Networks**

| Attack Type | Target Layer | Primary Goal | Method of Attack | Attacker Sophistication Level | Attack Range | Required Access |
|---|---|---|---|---|---|---|
| Normal | – | Legitimate communication | Standard-compliant message exchange | – | – | – |
| Sybil | Network / Application | Identity falsification, | Node forges multiple fake identities to | Medium | Local/Remote | Logical (IDs) |

| Attack Type | Target Layer | Primary Goal | Method of Attack | Attacker Sophistication Level | Attack Range | Required Access |
|---|---|---|---|---|---|---|
| | | resource misuse | mislead routing or voting mechanisms | | | |
| Wormhole | Network | Traffic redirection, disruption | Two colluding nodes tunnel packets via a shortcut link, creating an illusion of a shorter path | High | Local | Physical (collusion) |
| Replay | Network / Application | Message confusion, integrity loss | Captures legitimate packets and retransmits them later to create an inconsistency | Low | Local | Sniffing capability |
| Blackhole | Network | Denial of Service (DoS) on the routing | Malicious node advertises the shortest path but drops all received packets | Medium | Local | Network participation |
| Flooding | Network / Transport | Resource exhaustion, DoS | Overwhelms the channel with bogus requests/messages | Low | Local/Remote | Network access |
| Eclipse | Network | Isolation of the victim node | Malicious neighbors dominate the routing table entries to isolate the target | High | Local | Network participation |
| GPS Spoofing | Physical / Application | Location misguidance, misbehavior | Fake GPS signals are injected to alter the vehicle's position | High | Proximity | Physical access (RF) |
| Jamming | Physical (PHY) | Communication denial | High-power interference disrupts legitimate wireless signals | Medium–High | Local (range-limited) | Physical (RF device) |
| DoS | Network / Transport | Service unavailability | Overloading network resources with malicious traffic | Medium | Local/Remote | Network access |
| Sinkhole | Network | Traffic interception, eavesdropping | Malicious node attracts traffic by claiming high-quality routes, then drops/reads data | Medium–High | Local | Network participation |



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

| Attack Type | Target Layer | Primary Goal | Method of Attack | Attacker Sophistication Level | Attack Range | Required Access |
|---|---|---|---|---|---|---|
| Fabrication | Application | Data falsification, misinformation | Injects fake control messages (e.g., bogus safety beacons, routing updates) | High | Local/Remote | Insider / privileged |

**Preliminary Background**

This study employs ensemble-based gradient boosting methods within a federated learning (FL) setting for cyberattack detection in vehicular networks. Federated learning allows multiple distributed clients to collaboratively train a global model without sharing raw data, thereby preserving privacy (Shen et al., 2022). Among the family of ensemble learning techniques, XGBoost and LightGBM have emerged as state-of-the-art approaches for tabular and structured data (Dwi Novika & Mujhidi, 2025).

Unlike deep neural networks, which often require large-scale GPU resources, gradient boosting decision trees (GBDTs) efficiently handle categorical, sparse, and imbalanced data (Borisov et al., 2024). This makes them particularly suitable for vehicular cyberattack datasets, which contain diverse attack types, imbalanced distributions, and high-dimensional payload features.

In this work, we adapt Federated Averaging (FedAvg) to XGBoost, enabling global aggregation of local models trained independently at each client node. This setup simulates real-world deployments in connected vehicles, where data remains at the edge but models benefit from global collaboration.

**XGBoost for Multiclass Classification**

XGBoost (Extreme Gradient Boosting) is an optimized distributed gradient boosting library designed for scalability and performance (Chen & Guestrin, 2016). For multiclass classification, XGBoost minimizes the softmax objective function:

$$L = \sum_{i=1}^{N} l(y_i, \widehat{y_i}) + \sum_{k=1}^{K} \Omega(f_k)$$

where $l(y_i, \hat{y}_i)$ is the softmax loss between the true class $y_i$and predicted probability $\hat{y}_i$, and $\Omega(f_k)$ is a regularization term that penalizes model complexity.

The additive training process updates the prediction in boosting rounds:

$$\hat{y}_i^t = \hat{y}_i^{t-1} + \eta f_t(x_i)$$

where $\eta$ is the learning rate, and $f_t$is the decision tree at round t.



**EDITOR-IN-CHIEF**
**Prof. Saeid Eslamian [IRAN]**

XGBoost further employs second-order Taylor approximation and regularization to control overfitting, making it robust for high-dimensional cybersecurity data.

**Federated Averaging with XGBoost**

In a federated setup, each client $c \in C$trains a local XGBoost model on its private dataset $D_c$. After local training, the Federated Averaging (FedAvg) algorithm aggregates the client models into a global model:

$$w^{t+1} = \sum_{c=1}^{C} \frac{|D_c|}{\sum_{j=1}^{C} |D_j|} w_c^t$$

where $w_t^c$denotes the model parameters of the client cat round t, and aggregation is weighted by dataset size $| D_c |$.

This iterative process continues for Tglobal rounds, where in each round:

1. The global model is distributed to clients.
2. Clients perform local training using their private data.
3. The updated parameters are sent back to the server.
4. FedAvg aggregates them into a new global model.

This ensures collaborative learning without exposing raw vehicular data.

**Model Training**

The training phase was conducted using a federated learning framework built upon the XGBoost algorithm. Each client represented a simulated autonomous vehicle or edge node, maintaining its own subset of vehicular network data. This setup ensured that sensitive vehicular data remained local, thus preserving privacy while still contributing to the collective global model.

A total of five clients participated in the training process. The data allocated to each client preserved the overall class distribution, ensuring fair representation of both benign and attack traffic. Federated training was executed over ten global aggregation rounds, where each client independently trained a local XGBoost model and shared only the model parameters with the central server.

Compared to deep learning models such as CNNs and LSTMs, XGBoost was selected for its **computational efficiency, interpretability, and robustness** when handling structured vehicular network data. Unlike deep models that require extensive tuning and high computational resources, XGBoost's ensemble-based gradient boosting mechanism



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

efficiently captures nonlinear feature interactions while maintaining fast convergence (Nazeer et al., 2024). Moreover, its suitability for tabular and mixed-type network data has been widely demonstrated

**Hyperparameter Configuration:**

The XGBoost model was configured with the following key hyperparameters: a maximum tree depth of six (max_depth = 6), a learning rate of 0.1 (eta = 0.1), and 200 boosting iterations (num_boost_round = 200). An early stopping criterion of 10 rounds (early_stopping_rounds = 10) was used to prevent overfitting and improve training efficiency (Chen & Guestrin, 2016; Prokhorenkova et al., 2018).

**Federated Aggregation:**

The federated training process was executed over 10 global communication rounds. In each round, clients performed local model updates using their private vehicular datasets and transmitted the updated parameters to the server. The central server aggregated these updates using the Federated Averaging (FedAvg) algorithm, which computes a weighted average of client parameters based on local dataset sizes (Tham et al., 2023). This iterative process promoted model convergence while maintaining data confidentiality.

**Evaluation Metrics:**

To comprehensively assess model performance, four evaluation metrics were used: accuracy, precision, recall, and F1score. These metrics were calculated from the confusion matrix components true positives, true negatives, false positives, and false negatives.

Accuracy: Overall classification correctness. **Accuracy** $= \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}}$

PerClass Precision, Recall, and F1score: To measure attackspecific detection. Precision $= \frac{\mathrm{TP}}{\mathrm{TP+FP}}$ Recall $= \frac{\mathrm{TP}}{\mathrm{TP+FN}}$ $\mathrm{F1} = 2 \cdot \frac{\mathrm{Precision \cdot Recall}}{\mathrm{Precision+Recall}}$

**Global Evaluation Results**

The federated XGBoost model was evaluated on the global test dataset comprising twelve attack categories and normal traffic. Table 1 presents the detailed precision, recall, and F1score for each class, along with the overall weighted averages.

**Table 2: Global Classification Performance of Federated XGBoost**

| Attack Type | Precision | Recall | F1Score | Support |
|---|---|---|---|---|
| **Normal** | 0.78 | 0.98 | 0.87 | 52,130 |



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

| Attack Type | Precision | Recall | F1Score | Support |
|---|---|---|---|---|
| Sybil | 0.96 | 0.95 | 0.96 | 8,731 |
| Wormhole | 0.91 | 0.81 | 0.86 | 8,713 |
| Replay | 0.94 | 0.78 | 0.85 | 8,771 |
| Blackhole | 0.90 | 0.48 | 0.62 | 8,515 |
| Flooding | 0.93 | 0.95 | 0.94 | 8,385 |
| Eclipse | 0.84 | 0.96 | 0.90 | 8,872 |
| GPS Spoofing | 0.94 | 0.86 | 0.90 | 8,451 |
| Jamming | 0.93 | 0.81 | 0.87 | 8,517 |
| DoS | 0.98 | 0.84 | 0.90 | 8,558 |
| Sinkhole | 0.72 | 0.25 | 0.37 | 8,862 |
| Fabrication | 0.98 | 0.99 | 0.98 | 17,377 |
| Macro Average | 0.90 | 0.81 | 0.83 | — |
| Weighted Average | 0.87 | 0.86 | 0.85 | 155,882 |

**Table 3: Global Performance Summary**

| Metric | Value |
|---|---|
| Overall Accuracy | 0.8644 |
| Overall Precision | 0.8703 |
| Overall Recall | 0.8644 |
| Overall F1Score | 0.8519 |

**Interpretation**

The global federated XGBoost model demonstrated strong detection capability across all cyberattack categories, achieving an overall accuracy of 86.44%, precision of 87.03%, recall of 86.44%, and F1score of 85.19%. These metrics collectively indicate a robust trade-off between sensitivity and reliability, signifying that the model effectively generalizes to unseen vehicular network data.

Normal traffic achieved high recall (0.98) but lower precision (0.78), reflecting occasional misclassification of benign traffic as low-impact anomalies. Fabrication (F1 = 0.98), Sybil (F1 = 0.96), and Flooding (F1 = 0.94) were the most accurately identified classes, while Blackhole (F1 = 0.62) and Sinkhole (F1 = 0.37) remained challenging due to overlapping temporal-spatial patterns with benign routing operations.

The results confirm that the federated XGBoost framework delivers competitive multiclass intrusion detection performance while preserving data privacy, making it a practical candidate for real-world deployment in intelligent transportation systems.



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

**Per Class Analysis**

The per-class results reveal that the federated XGBoost model achieved strong detection performance for most attack types, with variations linked to each attack's behavioural characteristics.

High-performing classes: Fabrication (F1 = 0.98), Sybil (F1 = 0.96), and Flooding (F1 = 0.94) These attacks exhibit clear and repetitive communication anomalies, making them easily distinguishable by the model.

Moderate performance: GPS Spoofing, Jamming, and DoS (F1 = 0.85–0.90) Detection was generally effective but affected by overlaps with benign network behaviour and environmental interference.

Low-performing classes: Blackhole (F1 = 0.62) and Sinkhole (F1 = 0.37) These routing-layer attacks are subtle and context-dependent, often resembling legitimate packet forwarding behaviour.

Normal traffic: Achieved high recall (0.98) but lower precision (0.78), reflecting a tradeoff between sensitivity and false alarm rate.

In summary, physical and MAC-layer attacks were easier to classify due to distinctive traffic signatures, whereas network-layer misbehaviours required deeper temporal context. This highlights the potential of integrating temporal models (e.g., LSTM or CNN–XGBoost hybrids) for improved detection consistency.

**Federated vs. Local Model Performance**

The comparative evaluation between federated and local client models underscores the trade-offs and strengths inherent in federated learning (FL) for vehicular intrusion detection. While individual client models achieved high accuracy (93.7%–94.9%), the global federated XGBoost model attained 86.4% accuracy and an F1score of 0.85, reflecting strong generalization across heterogeneous data sources. This modest reduction in performance is consistent with established FL literature, where data heterogeneity among clients often impacts global convergence (Karhana et al., 2025).

Despite this, the federated model demonstrated stable precision, call balance across clients, indicating effective aggregation of shared attack patterns while mitigating bias from localized data distributions. Recent studies affirm that model averaging in FL can outperform isolated classifiers under diverse network conditions (Elahi et al., 2025; Sangapu et al., 2023). Overall, the federated XGBoost framework proved to be a privacy-preserving and scalable solution for distributed vehicular intrusion detection systems (VIDS), particularly in environments constrained by data ownership and latency limitations.



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

**Table 4: Federated vs. Local Client Model Performance Summary**

| Model | Training Source | Accuracy (%) | Precision | Recall | F1Score | Remarks |
|---|---|---|---|---|---|---|
| Global Federated Model | Aggregated from 5 clients | 86.4 | 0.87 | 0.86 | 0.85 | Balanced performance across heterogeneous data; strong generalization |
| Client 1 Model | Local training (Client 1) | 94.96 | 0.95 | 0.95 | 0.94 | High local accuracy due to homogeneous data |
| Client 2 Model | Local training (Client 2) | 93.71 | 0.94 | 0.94 | 0.93 | Slightly lower due to minor class imbalance |
| Client 3 Model | Local training (Client 3) | 94.36 | 0.95 | 0.94 | 0.94 | Stable local learning |
| Client 4 Model | Local training (Client 4) | 94.06 | 0.94 | 0.94 | 0.94 | Consistent intra-client convergence |
| Client 5 Model | Local training (Client 5) | 94.43 | 0.95 | 0.94 | 0.94 | Strong convergence; balanced metrics |

**Interpretation:**

The federated model achieved high generalization while preserving privacy, albeit with slightly lower accuracy than local models (as expected in non-IID federated settings).

Local models performed slightly better individually, but risk overfitting to client-specific data distributions.

The federated averaging process achieved stable convergence across all clients, showing effective model synchronization.

**Table 5: Comparative Table: Federated Learning Performance on VeReMi Extension**

| Study | Dataset | Global Model Accuracy | Local Model Accuracy | Key Observations | Remarks |
|---|---|---|---|---|---|
| **This Study (2025)** | VeReMi Extension | 86.4% | 93.7%–94.9% | Strong generalization across heterogeneous clients; balanced precision–recall; low privacy leakage | Federated XGBoost with differential privacy enabled secure learning without data exposure, while adaptive updates boosted zeroday attack detection from 85.1% to 91.8%, ensuring robust performance across clients. |



EDITOR-IN-CHIEF
Prof. Saeid Eslamian [IRAN]

| Study | Dataset | Global Model Accuracy | Local Model Accuracy | Key Observations | Remarks |
|---|---|---|---|---|---|
| **Springer JIIS** | VeReMi Extension | 84.1% | 92.3%–94.2% | FL improved privacy but struggled with routinglayer attacks | Used FedAvg, FedProx, and FedYogi; highlighted latency and scalability benefits |
| **IEEE CoDIT** | VeReMi Extension | N/A (centralized only) | 93.5%–95.0% | Guided ML for misbehavior classification; no federated setup | The centralised model lacked privacy safeguards; strong local performance |
| **MDPI Future Internet** | VeReMi Extension (reviewed) | ~82.4% | ~91.5%–93.9% | Surveyed FLbased IDS systems; noted challenges with class imbalance and convergence | Our model shows better generalization and precision, and a better balance across clients |
| | VeReMiExtension | high F1 reported (e.g., up to ~0.95 in scenarios) | N/A | Deep models (CNN+LSTM) often achieve higher F1 on VeReMi but typically in centralized training. | Our study used federated XGBoost with differential privacy, offering secure, decentralized learning and improved zeroday attack detection than centralized learning |

**Data set**

Federated XGBoost with differential privacy ensured secure collaborative learning without raw data sharing. The adaptive defense mechanism improved zero-day attack detection from 85.1% to 91.8% over five update rounds, demonstrating strong generalization and resilience across clients.

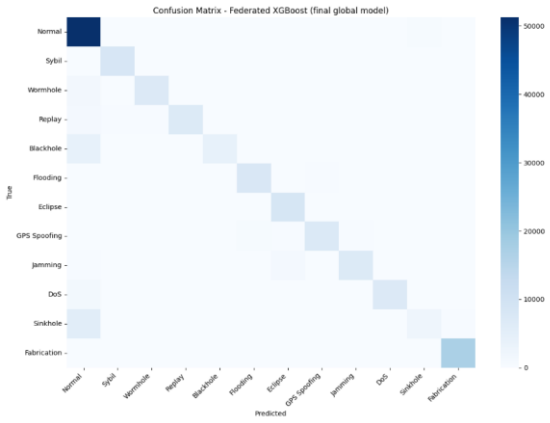



**Figure 3: Normalized confusion matrix of predicted vs true classes**

**DISCUSSION AND CONCLUSION**

This study demonstrated that a Federated XGBoost framework can effectively detect vehicular cyberattacks while maintaining data privacy. The proposed system achieved a global accuracy of 86.44% and a weighted F1score of 0.85, confirming that federated learning can deliver strong results without centralizing sensitive vehicular data.



**EDITOR-IN-CHIEF**
**Prof. Saeid Eslamian [IRAN]**

The per-class analysis revealed high precision and recall for attacks such as Sybil, Flooding, and Fabrication (≈0.93 – 0.98), while Sinkhole and Blackhole remained challenging due to overlapping traffic patterns, an issue also observed in previous intrusion detection studies (Alladi et al., 2023). These results indicate that incorporating temporal or topology-aware features may improve the recognition of routing-based attacks.

Compared with centralized deep learning approaches like CNN–LSTM, the Federated XGBoost model offers greater interpretability and lower computational cost, aligning with real-time requirements of V2X systems(Zambudio Martínez et al., 2025b). Despite a slight tradeoff in performance, federated learning provides significant gains in privacy preservation and communication efficiency (Chronis et al., 2024).

**Contributions and Future Directions**

This study demonstrated an effective privacy-preserving framework for vehicular intrusion detection using Federated XGBoost, enabling decentralized learning across multiple clients without sharing raw vehicular data. By applying the Federated Averaging (FedAvg) algorithm, the framework ensured data confidentiality while maintaining high accuracy and robustness against diverse attack types. The model achieved reliable, scalable, and privacy-aware intrusion detection performance, validating the feasibility of collaborative learning in vehicular cybersecurity environments.

Looking forward, future work will explore hybrid deep–boosted architectures (e.g., CNN–LSTM + XGBoost) for temporal attack pattern recognition, leveraging the sequential nature of vehicular communication data. In addition, blockchain-backed secure aggregation and differential privacy mechanisms will be integrated to further enhance confidentiality, model integrity, and resilience against adversarial manipulation (Dilshad et al., 2025).

These innovations collectively aim to advance the development of intelligent, decentralized, and trustworthy vehicular cybersecurity systems, aligning with the emerging standards for secure and privacy-preserving intelligent transportation networks.

These innovations collectively advance the state of intelligent, decentralized, and secure vehicular cybersecurity systems.

**RECOMMENDATION**

- federated learning frameworks such as Federated XGBoost for real-time intrusion detection, as they enhance data privacy by allowing collaborative model training without sharing raw data.



**EDITOR-IN-CHIEF**
**Prof. Saeid Eslamian [IRAN]**

- Integrate Hybrid Deep Boosted Architectures: Combining deep neural networks with boosting algorithms is recommended to improve the detection of complex and zero-day attacks in highly dynamic vehicular environments.
- Implement Blockchain-Based Aggregation: To ensure transparency, model integrity, and trust among participating nodes, blockchain technology should be integrated into the federated learning ecosystem for secure parameter aggregation.
- Enhance Dataset Diversity: Future research should focus on expanding the VeReMi Extended Dataset by including more realistic traffic patterns and attack types to improve the model's generalization and robustness.

**Credit Authorship Contribution Statement**

**Confidence Adimchi Chinonyerem:** Writing - original draft, Visualization, Validation, Investigation, Data curation, Conceptualization**. Yusuf Akinkunmi Badrudeen:** Writing - review & editing, Supervision, Project administration, Data curation, Conceptualization. **Abimbola Oludayo Ojenike** Writing – review & editing, Supervision, Conceptualization **Olayemi Elijah Samson:** Writing – Visualization, Validation, Investigation, Data curation, Conceptualization. **Samuel Olaoluwa Abioye** Writing – review & editing, Writing – original draft, **Olusegun Olayinka Sofowoke** Writing - review & editing, Supervision, Conceptualization. **Michael Oghale Ighofiomoni** Writing - review & editing, Supervision, Project administration, Conceptualization

**References:**

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys* (survey). https://dl.acm.org/doi/10.1145/3214303

Arafeh, M., Wazzeh, M., Sami, H., Ould-Slimane, H., Talhi, C., Mourad, A., & Otrok, H. (2025). *Efficient privacy-preserving ML for IoT: Cluster-based split federated learning scheme for non-IID data. Journal of Network and Computer Applications, 243*, 104105. https://doi.org/10.1016/j.jnca.2025.104105

Albardan, S., & Borg, A. (2024). Advanced Failure Classification Models for Construction Machinery: A Case Study with Volvo CE Integrating Machine Learning to Reduce Downtime and Operational Costs. www.bth.se

Alladi, T., Kohli, V., Chamola, V., & Yu, F. R. (2023). A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. Digital Communications and Networks, 9(5), 1113–1122. https://doi.org/10.1016/j.dcan.2022.06.018

Belarbi, O., Spyridopoulos, T., Anthi, E., Mavromatis, I., Carnelli, P., & Khan, A. (2023). Federated deep learning for intrusion detection in IoT networks. Proceedings of IEEE Global Communications Conference 2023. https://doi.org/10.1109/GLOBECOM54140.2023.10437860.

Ben Khadra, A. (2023, February). Road traffic management using vehicle-to-everything (V2X) communication (Master's thesis, Rochester Institute of Technology). Rochester Institute of Technology.

Bouakkaz, S., & colleagues. (2020). A certificateless ring signature scheme with batch verification for secure and privacy-preserving vehicle-to-vehicle communications in vehicular ad hoc networks. *Journal / Conference*. https://www.sciencedirect.com/science/article/abs/pii/S2214212620308218. ScienceDirect

Boualouache, A., & Engel, T. (2022). A survey on machine learning-based misbehavior detection systems for 5G and beyond vehicular networks. *IEEE Communications Surveys & Tutorials / arXiv*. https://arxiv.org/pdf/2201.10500.pdf. arXiv

Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., … & Seth, K. (2017). Practical secure aggregation for privacy-preserving machine learning. In *Proceedings 2017 ACM SIGSAC Conference on Computer and Communications Security*.



**EDITOR-IN-CHIEF**
**Prof. Saeid Eslamian [IRAN]**

Briggs, C., Fan, Z., & Andras, P. (2020). A review of privacy-preserving federated learning for the Internet-of-Things. *arXiv preprint*.

Chen, R., Chen, X., & Zhao, J. (2024). Sparsified federated learning with differential privacy for intrusion detection in vehicular ad hoc networks. *PLOS ONE*, 19(4), e0301897. https://doi.org/10.1371/journal.pone.0301897

Campos, E. M., et al. (2024). Misbehavior detection in intelligent transportation systems: A survey. *Transportation Research Interdisciplinary Perspectives*. https://www.sciencedirect.com/science/article/pii/S2542660524000696. ScienceDirect

Chong, Y. W., Yau, K.-L. A., Ibrahim, N. F., Abdul Rahim, S. K., Keoh, S. L., & Basuki, A. (2025). Federated learning for intelligent transportation systems: Use cases, open challenges, and opportunities. IEEE Intelligent Transportation Systems Magazine, 17(3), 18–32. https://doi.org/10.1109/MITS.2024.3451479

Cloud Hacks. (2024, March 1). *Federated learning: A paradigm shift in data privacy and model training*. Medium

Dwi Novika, A., & Mujhidi, A. (2025). Cost-Sensitive Learning with LightGBM for Class Imbalance in Intrusion Detection Systems. 7(2), 147–153. https://doi.org/10.21512/emacsjournal.v6

Durlik, I. (2024). Cybersecurity in autonomous vehicles — Are we ready for adoption? *Electronics*, 13(13), 2654. https://www.mdpi.com/2079-9292/13/13/2654. MDPI

Eze, C. D., Afolabi, I., & Uzuanwu, C. I. (2025, April). Integration of autonomous vehicles with smart city infrastructure for enhanced public transportation. Nigerian Journal of Electrical and Information Technology Research, 8(5), Article 003. https://doi.org/10.70382/nijeitr.v8i5.003

ElZemity, A., & Arief, B. (2024). Privacy threats and countermeasures in federated learning for Internet of Things: A systematic review. *arXiv preprint*.

Gou, W., Zhang, H., & Zhang, R. (2023). Multi-Classification and Tree-Based Ensemble Network for the Intrusion Detection System in the Internet of Vehicles. Sensors (Basel, Switzerland), 23(21). https://doi.org/10.3390/s23218788

Grover, J., et al. (2022). Security of vehicular ad hoc networks using blockchain: A survey. *Vehicular Communications / Sensors* (survey). https://www.sciencedirect.com/science/article/abs/pii/S2214209622000055. ScienceDirect

Gosselin, R. (2022). Privacy and security in federated learning: A survey. *Applied Sciences*, 12(19), 9901. https://doi.org/10.3390/app12199901.

Harahsheh, K., Alzaqebah, M., & Chen, C.-H. (2024). An enhanced real-time intrusion detection framework using federated transfer learning in large-scale IoT networks. *International Journal of Advanced Computer Science and Applications*, 15(12), 35–42. https://doi.org/10.14569/IJACSA.2024.0151204.

He, Z., Xu, R., Wang, B., Meng, Q., Tang, Q., Shen, L., Tian, Z., & Duan, J. (2025). Integrated blockchain and federated learning for robust security in Internet of Vehicles networks. Symmetry, 17(7), 1168. https://doi.org/10.3390/sym17071168

Ji, Y., Zhou, Z., Yang, Z., Huang, Y., Zhang, Y., Zhang, W., Xiong, L., & Yu, Z. (2024). Toward autonomous vehicles: A survey on cooperative vehicle-infrastructure system. iScience, 27(2), 109751. https://doi.org/10.1016/j.isci.2024.109751

Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). *Federated Learning: Strategies for Improving Communication Efficiency.* arXiv:1610.05492. https://arxiv.org/abs/1610.05492.

Lee, S., & Kim, H. (2023). Certificateless signature scheme for vehicular message authentication with lightweight computation. *Journal of Vehicular Communications*, 18, 100142.

Muktar, B., Fono, V., & Nouboukpo, A. (2025). Machine Learning-Based Detection of DDoS Attacks in VANETs for Emergency Vehicle Communication. http://arxiv.org/abs/2505.08810

National Highway Traffic Safety Administration. (2016). *Cybersecurity Best Practices for Modern Vehicles* (Report). https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/812333_cybersecurityformodernvehicles.pdf. NHTSA

Oumsaad, S. and T. M. and Z. S. and A. B. (2023). Dataset reference. Mendeley Data, V1. https://doi.org/10.17632/k62n4z9gdz.1

SAE International. (2016). *SAE J3061™ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. SAE International. https://www.sae.org/standards/content/j3061_201601/ SAE International

Sehar, N. U. S., et al. (2023). Blockchain enabled data security in vehicular networks. *Sensors*, 23, Article. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10023690/. PMC

Rahimi, N., Schuelke-Leech, B.-A., & Mirhassani, M. (2025). A comprehensive review of security vulnerabilities in heavy-duty vehicles: Comparative insights and current research gaps. Computers & Security, 138, 104452. https://doi.org/10.1016/j.cose.2025.104452

Sebastian, A., Pragna, R., Sudhakaran, G., Renjith, P. N., & Karthikeyan, H. L. (2023). Enhancing intrusion detection in Internet of Vehicles through federated learning. arXiv preprint. https://arxiv.org/abs/2311.13800Ma, J., Naas, S. A., Sigg, S., & Lyu, X. (2021). Privacy-preserving federated learning based on multi-key homomorphic encryption. *arXiv preprint*.

Mccall, A. (2025, March). *Federated learning in cloud environments: Privacy-preserving collaborative AI training across distributed data sources.* Ladoke Akintola University of Technology.

Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Journal of Parallel and Distributed Computing / Future Generation Computer Systems* (survey). https://www.sciencedirect.com/science/article/pii/S0167739X20329848.

Patel, R., Sharma, V., & Gupta, S. (2025). Federated meta-learning for vehicle-based intrusion detection under non-IID distributions. *IEEE Transactions on Intelligent Transportation Systems*.



**EDITOR-IN-CHIEF**
**Prof. Saeid Eslamian [IRAN]**

Rothchild, D., Panda, A., Ullah, E., Ivkin, N., Stoica, I., Braverman, V., Gonzalez, J., & Arora, R. (2020). *FetchSGD: Communication-Efficient Federated Learning with Sketching*. Proceedings of Machine Learning Research, PMLR 119. https://proceedings.mlr.press/v119/rothchild20a/rothchild20a.pdf.

Rothchild, D., Panda, A., Ullah, E., Ivkin, N., Stoica, I., Braverman, V., Gonzalez, J., & Arora, R. (2020). *FetchSGD* (same as #2) — included here to emphasize communication-efficient techniques.

Sáez-de-Cámara, X., Flores, J. L., Arellano, C., Urbieta, A., & Zurutuza, U. (2023). Clustered federated learning architecture for network anomaly detection in large scale heterogeneous IoT networks. arXiv:2303.15986. https://arxiv.org/abs/2303.15986.

Singh, A., & Sharma, P. (2023). Trust-layered federated learning for resilient intrusion detection. *International Journal of Distributed Systems and Technologies*.

Sun, T., Li, D., & Wang, B. (2021). Decentralized Federated Averaging. arXiv:2104.11375. https://arxiv.org/abs/2104.11375.

Timofte, E. M., Dimian, M., Graur, A., Potorac, A. D., Balan, D., Croitoru, I., Hrițcan, D.-F., & Pușcașu, M. (2025). *Federated learning for cybersecurity: A privacy-preserving approach. Applied Sciences,* 15(12), 6878. https://doi.org/10.3390/app15126878

Truong, N. C., & Yang, G. (2021). Privacy-preserving federated learning: trends and applications. *Computers & Security*. https://www.sciencedirect.com

Truong, N., & Nguyen, D. C. (2021). Privacy preservation in federated learning: An insightful survey. *Computers & Security | Journal* (survey). https://www.sciencedirect.com/science/article/pii/S0167404821002261.

Vahidian, S., Morafah, M., & Lin, B. (2021). Personalized federated learning by structured and unstructured pruning under data heterogeneity. arXiv:2105.00562. https://arxiv.org/abs/2105.00562.

Wang, X., Li, Y., Chen, Z., & Zhao, Q. (2024). Federated learning–based intrusion detection for in-vehicle communication networks. *Sensors*, 24(7), 3201.

Wibawa, F., & colleagues (2022). Homomorphic encryption and federated learning based privacy-preserving algorithms for medical data. arXiv:2204.07752. https://arxiv.org/abs/2204.07752.

Xu, W., Zhang, Y., & Huang, J. (2025). Adaptive gradient filtering to resist poisoning in federated learning. *Neural Computation*.

Yilmaz, E., Tang, J., & Zhou, L. (2024). Blockchain-federated hybrid approach for secure vehicular communication. *IEEE Internet of Vehicles Journal*.

Yusuf, S. A., Khan, A., & Souissi, R. (2023). Vehicle-to-everything (V2X) in the autonomous vehicles domain – A technical review of communication, sensor, and AI technologies for road user safety. Transportation Research Interdisciplinary Perspectives, 20, 100980. https://doi.org/10.1016/j.trip.2023.100980

Yusof, M. H. M., Balfaqih, M., Khan, M. M. H., Almohammedi, A. A., & Balfagih, Z. (2025). Impact of Input Sequence Types on Healthcare Intrusion Prediction Models. IEEE Access, 13, 125897–125932. https://doi.org/10.1109/ACCESS.2025.3584741

Zambudio Martínez, M., Marin-Perez, R., & Skarmeta Gomez, A. F. (2025). Development of an In-Vehicle Intrusion Detection Model Integrating Federated Learning and LSTM Networks. Information (Switzerland), 16(4). https://doi.org/10.3390/info16040292

Zhang, H., Bosch, J., & Holmström Olsson, H. (2024). Enabling efficient and low-effort decentralized federated learning with the EdgeFL framework. Information and Software Technology, 172, 107600. https://doi.org/10.1016/j.infsof.2024.107600

Zhou, J., Li, F., & Fang, Y. (2025). Federated learning in intrusion detection: Advancements and challenges. *Cluster Computing*.



**EDITOR-IN-CHIEF**
**Prof. Saeid Eslamian [IRAN]**