SECURITY AND PRIVACY

Research Article

Enhancing VANET Security Using a Hybrid Model of Deep Learning and Homomorphic Encryption

Submission ID 77cacfc7-ebda-40fa-94a3-f5f16c72232f

Submission Version Initial Submission

PDF Generation 24 Aug 2025 06:32:40 EST by Atypon ReX

Authors

Haythem Hayouni
Corresponding Author
Submitting Author

ORCiD
https://orcid.org/0000-0003-3340-6165

Affiliations

- IT Department, Higher Institute of Computer Science, Tunisia

Additional Information

Keywords

Communication Security / Authentication

Authentication

Communication Security / Cryptography

Cryptography

Communication Security / Denial of service prevention schemes for communication systems

Denial of service prevention schemes for communication systems

Research Topics

Communication Security

Files for peer review

All files submitted by the author for peer review are listed below. Files that could not be converted to PDF are indicated; reviewers are able to access them online.

Name	Type of File	Size	Page
Manuscript.pdf	Main Document - LaTeX PDF	975.7 KB	Page 3

Enhancing VANET Security Using a Hybrid Model of Deep Learning and Homomorphic Encryption

Haythem Hayouni

IT Department, Higher Institute of Computer Science, Tunisia
hayouni.haythem.isi@gmail.com

Abstract: Vehicular Ad Hoc Networks (VANETs) are characterized by their highly dynamic and decentralized architecture, which makes them susceptible to various cyber threats such as Sybil attacks, black hole attacks, and message spoofing. In this paper, we propose, HyDra-VANET, a novel hybrid framework that combines the strengths of deep learning and homomorphic encryption to ensure robust and privacy-preserving intrusion detection in VANET environments. Our approach utilizes a convolutional-recurrent neural network (CRNN) to extract temporal and spatial features from vehicular communication data in real-time. To preserve driver and vehicle privacy, all sensitive data are encrypted using a lightweight lattice-based homomorphic encryption scheme, allowing encrypted inference and collaborative model training without exposing raw data. The proposed system is evaluated using a combination of real-world VANET traffic datasets and simulated adversarial scenarios. The framework significantly outperforms traditional IDS approaches in both detection capability, data confidentiality, and privacy-conscious vehicular communication systems.

Keywords: VANET Security; Intrusion Detection System (IDS); Federated Learning; Homomorphic Encryption; Deep Learning.

1 Introduction

Intelligent Transportation Systems (ITS) are revolutionizing mobility by integrating real-time data processing, communication technologies, and artificial intelligence to enable safer and more efficient traffic systems. At the core of this transformation lies the Vehicular Ad Hoc Network (VANET), a specialized subclass of Mobile Ad Hoc Networks (MANETs) that enables communication between vehicles (V2V) and between vehicles and infrastructure (V2I) [1,2]. Through VANETs, vehicles can share information on road conditions, traffic density, accidents, and more, thereby improving road safety and traffic efficiency. Despite these advantages, VANETs face significant security and privacy challenges. Due to their open wireless communication channels, high mobility, and dynamic topologies, VANETs are inherently vulnerable to a wide range of attacks such as Sybil attacks, black hole attacks, denial of service (DoS), and message tampering. Traditional cryptographic methods, while necessary, are often insufficient to provide proactive threat detection or to protect against internal compromised nodes. Moreover, intrusion detection systems (IDSs) [3] based on

rule-based or shallow machine learning techniques often suffer from high false-positive rates and limited adaptability to new or evolving threats.

To address these issues, we propose HyDra-VANET a novel hybrid framework that combines deep learning-based intrusion detection with homomorphic encryption to deliver both accurate threat detection and strong privacy guarantees. By using deep neural networks, the system can autonomously learn complex patterns of malicious behavior from raw network traffic. Simultaneously, with the integration of homomorphic encryption [6,7], data privacy is preserved throughout the detection pipeline, ensuring that sensitive vehicle data never needs to be decrypted during processing or model training.

1.1 Motivation

The rapid adoption of connected vehicles and the growth of intelligent transportation systems have introduced new challenges in terms of cybersecurity and data privacy. VANETs are highly dynamic environments where vehicles continuously broadcast information such as location, speed, braking status, and more. While this data exchange enables real-time decision-making and improves road safety, it also exposes vehicles to critical security vulnerabilities. Common threats in VANETs include:: *Sybil Attacks*, where a single malicious node claims multiple fake identities to manipulate network behavior, *Black Hole Attacks*, where a node absorbs data packets without forwarding them, *Message Tampering*, where attackers alter or forge traffic data to mislead surrounding vehicles, and *Eavesdropping and Tracking*, which infringe on user privacy and could lead to profiling or surveillance. Traditional security approaches based on signature-based detection or rule-based filtering struggle in these environments due to their limited adaptability and high false positive rates. Moreover, centralized IDS architectures require raw data to be sent to external servers, creating single points of failure and serious privacy risks. On the other hand, deep learning models [4,5] especially those based on temporal and spatial feature learning have demonstrated exceptional capabilities in recognizing complex patterns in time-series network traffic. However, integrating deep learning into real-world VANET systems raises a significant challenge: ensuring that sensitive vehicle data is not exposed during model training or inference. This is where homomorphic encryption (HE) comes into play. HE enables computation over encrypted data, meaning that even untrusted devices or servers can participate in data processing without ever seeing the original data. Recent advances in lattice-based HE schemes have made such systems increasingly practical, even in constrained environments like vehicles.

The motivation behind HyDra-VANET is to bridge the gap between these two domains leveraging deep learning for intelligent intrusion detection while using homomorphic encryption to enforce data privacy. The goal is to build a next-generation security system for VANETs that is accurate, efficient, and privacy-preserving, even in highly adversarial settings.

1.2 Main Contributions

This paper introduces HyDra-VANET, a hybrid architecture that integrates deep learning and homomorphic encryption to provide a comprehensive solution to intrusion detection in VANETs. Our primary contributions are summarized below:

- Design of an efficient framework with a hybrid security architecture that fuses the strengths of two emerging technologies:

- A Convolutional-Recurrent Neural Network (CRNN) for efficient feature extraction from high-dimensional and temporal VANET traffic data.

- A lattice-based Homomorphic Encryption (HE) scheme that allows the system to operate entirely on encrypted data during both training and inference.

- Privacy-Preserving Encrypted Inference Pipeline: We implement an encrypted inference mechanism that enables real-time threat detection without revealing sensitive vehicle data at any stage. Unlike federated learning or differential privacy, our approach ensures that raw data remains encrypted end-to-end, offering a higher level of privacy protection.
- Adaptive Encryption-Aware Training Strategy: To optimize performance for real-world vehicular hardware (e.g., On-Board Units), we introduce an encryption-aware training pipeline. This pipeline adjusts model complexity and encryption parameters dynamically to balance detection accuracy and computational efficiency, making the system scalable and deployable.
- Comprehensive Evaluation on Realistic Datasets: We evaluate HyDra-VANET using both synthetic and real-world VANET intrusion datasets. Our experiments cover a wide range of attacks and mobility patterns.
- Comparative Analysis with Baselines: We benchmark our solution against traditional intrusion detection methods, including SVMs, random forests, and conventional neural networks without encryption.

The remainder of this paper is organized as follows. Section 2 reviews existing work on VANET security, deep learning for IDS, and privacy-preserving computation. Section 3 describes the architecture of VANETs, assumptions, and the adversary model considered in this study. Section 4 details the hybrid architecture, including the neural network model, encryption scheme, and training methodology. Section 5 presents the datasets, metrics, and evaluation results of the proposed model with a discussion. Section 6 summarizes the findings and outlines future directions.

2 Related Works

The security and privacy challenges in Vehicular Ad Hoc Networks (VANETs) have garnered significant research attention. Various approaches have been proposed, leveraging deep learning, homomorphic encryption (HE), and federated learning (FL) to enhance intrusion detection systems (IDS). This section categorizes and discusses some recent studies based on their core methodologies and contributions.

2.1 Deep Learning-Based Intrusion Detection

Deep learning techniques have been extensively applied to IDS in VANETs, offering robust mechanisms to detect complex and evolving cyber threats.

In [8], the authors proposed a machine learning-based cryptographic protocol for intrusion detection in V2X communications within VANETs. Their approach, termed ML-CPIDS, integrates advanced cryptographic protocols with machine learning to provide robust authentication, encryption, and real-time threat detection. The system addresses

significant security concerns such as eavesdropping, data manipulation, and unauthorized vehicle monitoring, enhancing the privacy and security of vehicular networks.

In [9], the authors introduced a hybrid deep learning model combining Self-Organizing Maps (SOMs), Deep Belief Networks (DBNs), and Autoencoders to detect cyber threats in IoT networks. Their model leverages Particle Swarm Optimization (PSO) for feature tuning, enhancing detection accuracy. Evaluated on datasets like NSL-KDD and CICIoT2023, the system demonstrated high accuracy and low false-positive rates, showcasing its effectiveness in identifying both known and emerging threats.

In [10], the authors developed VAN-IDS, a federated learning-based intrusion detection system tailored for VANETs. By combining packet-based and physics-based IDSs through Dempster-Shafer Theory (DST), the system achieves swift and efficient intrusion detection. VAN-IDS addresses the need for real-time threat detection in vehicular networks, ensuring both speed and accuracy in identifying potential attacks.

In [11], the authors proposed a federated learning-based IDS to enhance privacy and security in Unmanned Aerial Vehicles (UAVs). Recognizing the challenges of centralized systems in Flying Ad Hoc Networks (FANETs), their FL-IDS reduces computation and storage costs for both clients and central servers. This decentralized approach is crucial for resource-constrained UAVs, ensuring efficient intrusion detection without compromising privacy.

2.2 Homomorphic Encryption for Secure IDS

Homomorphic encryption (HE) enables computations on encrypted data, preserving privacy without compromising functionality. Several studies have integrated HE into IDS to enhance data confidentiality.

In [12], the authors explored the application of homomorphic encryption in machine learning for IoT and cloud environments. Their research focuses on developing innovative solutions that enhance data security using machine learning techniques. By integrating HE, they aim to process encrypted data without decryption, ensuring privacy in sensitive applications.

In [13], the authors proposed a privacy-preserving cyberattack detection framework for blockchain-based IoT systems. Their approach deploys AI-driven detection modules at blockchain nodes to identify real-time attacks. To safeguard privacy, data is encrypted using HE before transmission to a cloud service provider for training. They introduced a SIMD-optimized homomorphic packing algorithm and a novel deep neural network training algorithm optimized for encrypted data. The system achieves detection accuracy comparable to unencrypted approaches, with minimal performance degradation.

In [14], the authors presented FLSSM, a federated learning storage security model enhanced with homomorphic encryption. FLSSM addresses challenges like computation efficiency, attack tracing, and contribution assessment in encrypted federated learning environments. By utilizing parallel aggregation, introducing trusted supervisory nodes, and implementing fair reward mechanisms, FLSSM enhances both the efficiency and security of federated learning models.

In [15], the authors introduced FedML-HE, an efficient homomorphic-encryption-based privacy-preserving federated learning system. By selectively encrypting sensitive parameters, FedML-HE significantly reduces computation and communication overheads during training. The system demonstrates considerable overhead reduction, particularly

for large models, making HE-based federated learning more practical for real-world applications.

2.3 Federated Learning for Privacy-Preserving IDS

Federated learning (FL) enables decentralized model training across multiple devices, preserving data privacy by keeping data localized. This approach is particularly beneficial for intrusion detection in distributed networks like VANETs.

In [16], the authors proposed a federated learning framework for zero-day attack detection in 5G and beyond V2X networks. Leveraging deep autoencoders trained on benign traffic patterns, their system detects anomalies indicative of novel attacks. The federated approach ensures data privacy by keeping data localized, reducing communication overhead, and enhancing the detection of previously unseen threats.

In [17], the authors addressed data privacy issues in federated learning-based IDS for resource-constrained Internet-of-Vehicles (IoV) networks. They proposed a framework that integrates homomorphic encryption with federated learning, allowing encrypted data to be processed without decryption. This approach ensures data privacy while accommodating the limited computational resources of IoV devices.

In [18], the authors explored federated deep learning for intrusion detection in IoT networks. Their approach addresses challenges related to data heterogeneity and limited computational resources. By employing federated learning, the system enables collaborative model training without sharing raw data, preserving privacy. The study demonstrates that their approach achieves performance comparable to centralized models, highlighting its potential for scalable and privacy-preserving intrusion detection.

In [19], the authors conducted a comprehensive review of advancements in securing federated learning with IDS. They examined various techniques, including neural networks and feature engineering, to detect malicious clients in federated learning environments. The study emphasizes the importance of incorporating privacy-preserving mechanisms and robust security protocols to protect against emerging threats in distributed networks.

2.4 Comparative Analysis and Discussion

The comparative analysis in Table 1 highlights the evolution of intrusion detection research in vehicular and IoT systems. Studies such as [8,9] emphasize traditional deep learning approaches that excel in threat recognition and model accuracy, yet lack provisions for protecting user data and accommodating decentralized deployment models. These models perform well in controlled environments and against known attack vectors but may fall short in real-world VANET scenarios where privacy, mobility, and distributed computation are essential. Meanwhile, works in [10,15] explore federated learning (FL) as a means to enhance data privacy and reduce communication overhead. These systems allow intrusion detection to occur across distributed nodes without centralizing sensitive data, an essential feature in vehicular or UAV-based networks. However, the absence of strong encryption mechanisms in these FL approaches leaves them vulnerable to model inversion and poisoning attacks, especially when adversaries can access shared gradients or parameter updates. Homomorphic encryption (HE) has emerged as a powerful tool to close this gap. Research in [11,12,14] demonstrates that HE can facilitate secure model training and inference without ever revealing plaintext data, thereby reinforcing trust in cloud-based or collaborative intrusion detection systems. Nevertheless, these HE-enabled systems

often struggle with computational overhead, latency, and scalability factors that are critical in high-speed, resource-constrained vehicular networks. Only a few studies [13] attempt to integrate HE and FL in a resource-aware context explicitly tailored for the Internet of Vehicles (IoV), showing promising directions for scalable, encrypted, and privacy-preserving IDS. Federated learning-focused works by in [16,18,19] delve into privacy-aware distributed detection and the defense against emerging threats such as zero-day attacks and malicious client behaviors. However, despite offering strong theoretical models, these studies often fall short in delivering real-time, VANET-specific solutions validated under realistic vehicular conditions. Some emphasize review or simulation-based analysis without end-to-end deployment considerations. Overall, while each study contributes a crucial piece to the IDS security puzzle whether in detection intelligence, encryption, or distributed architecture there remains a clear absence of a unified framework that effectively combines deep learning's adaptability, homomorphic encryption's privacy guarantees, and federated learning's decentralized intelligence, all within the latency-sensitive and mobility-heavy context of VANETs.

This gap strongly motivates the development of a hybrid, end-to-end architecture like HyDra-VANET. By integrating deep learning, homomorphic encryption, and federated learning into a single framework tailored for VANETs, HyDra-VANET aspires to achieve high detection accuracy, robust privacy preservation, and distributed scalability without compromising computational feasibility. As the reviewed studies reveal, the convergence of these technologies though explored in parts remains an open challenge, one that HyDra-VANET seeks to address comprehensively.

Table 1: Comparison of IDS Techniques: Features, Advantages, and Limitations

Study	**DL**	**HE**	**FL**	**Privacy**	**VANET**	**Advantages**	**Limitations**
[8]	✓	×	×	✓	✓	Lightweight IDS using ML and cryptographic protocols; good for V2X environments	No homomorphic encryption or FL; centralized training
[9]	✓	×	×	×	×	Hybrid DL with SOMs, DBNs, Autoencoders; high accuracy	Lacks privacy and decentralization; not tailored for VANETs
[10]	✓	×	✓	✓	✓	Real-time VANET IDS using FL and DST; handles mobility well	No encryption; security limited to data locality
[11]	✓	×	✓	✓	×	Lightweight FL-IDS for UAVs; low communication overhead	Not designed for VANETs; lacks encryption
[12]	✓	✓	×	✓	×	Secure ML inference using HE; enhances data privacy	No federated learning; higher encryption latency
[13]	✓	✓	✓	✓	×	Combines blockchain, AI, FL, HE; strong privacy design	Complex system; not validated in VANET

[14]	×	✓	✓	✓	×	Efficient HE aggregation; attacker tracing	Lacks DL; general-purpose system not tailored for VANETs
[15]	✓	✓	✓	✓	×	Reduces HE overhead in FL; selective encryption of parameters	Not validated in vehicular context; computational tradeoffs
[16]	✓	×	✓	✓	✓	Detects zero-day attacks using FL and deep autoencoders	No encryption; only suitable for 5G-enabled scenarios
[17]	✓	✓	✓	✓	✓	Fully encrypted FL for IoV; suitable for low-resource devices	Encrypted operations introduce latency and overhead
[18]	✓	×	✓	✓	×	Handles data heterogeneity in IoT; accurate FL training	Not directly applicable to VANET; needs adaptation
[19]	✓	✓	✓	✓	✓	Rich review of FL+IDS integration; highlights key trust/security issues	Survey paper; lacks experimental system validation

3 System Architecture and Threat Model

This section presents the architecture of the Vehicular Ad Hoc Network (VANET) system studied in this work, outlines the key operational assumptions, and defines the adversary model used to evaluate the proposed intrusion detection approach.

3.1 VANET System Architecture

The VANET architecture considered in this study consists of three primary components: vehicles, roadside units (RSUs), and a central authority supported by edge computing infrastructure. Figure 1 presents a comprehensive architectural model of a Vehicular Ad Hoc Network (VANET) integrated with intelligent security mechanisms, namely deep learning, federated learning, and homomorphic encryption. The architecture is composed of three primary layers: the vehicular layer (vehicles), the infrastructure layer (RSUs and edge servers), and the control layer (central authority or cloud system).

- At the vehicular layer, each vehicle is equipped with an On-Board Unit (OBU), which serves as a smart computational node. OBUs are responsible for sensing the environment, collecting traffic and behavioral data, running local intrusion detection models, and participating in real-time Vehicle-to-Vehicle (V2V) communication. Vehicles also broadcast and receive periodic messages such as Basic Safety Messages (BSMs) and Cooperative Awareness Messages (CAMs), which are essential for safety-critical functions.
- The infrastructure layer includes Roadside Units (RSUs) that act as semi-trusted relay nodes. These RSUs facilitate Vehicle-to-Infrastructure (V2I) communication,

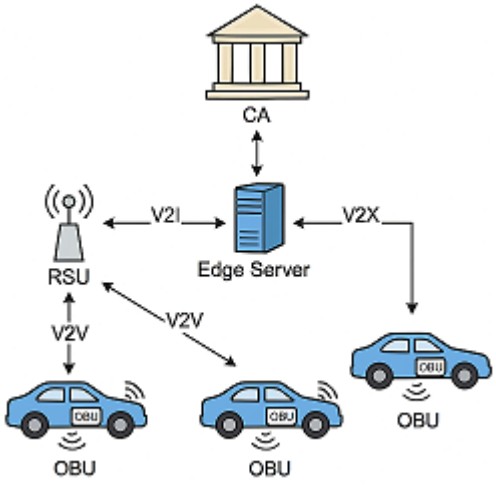

Figure 1: VANET System Architecture

aggregating encrypted model updates from multiple OBUs and forwarding them to the edge server or central authority. The RSUs also distribute model parameters, receive security updates, and support the initial setup of federated learning rounds.

- Edge servers and cloud components reside at the control layer. This layer is responsible for g odel aggregation, system-wide policy enforcement, cryptographic credential management, and coordination of privacy-preserving mechanisms. The central server oversees the orchestration of the federated learning process, including the selection of participating nodes, model versioning, and handling of encrypted updates using homomorphic encryption. This allows secure computation on encrypted data, ensuring that sensitive vehicular information is never exposed in plaintext form, even during analysis and training.

The figure also illustrates various communication paths: V2V, V2I, and V2C (Vehicle-to-Cloud), all of which are encrypted to ensure data integrity and confidentiality. The integration of federated learning allows each vehicle to train an IDS model locally, contributing to a global model without sharing raw data. Homomorphic encryption ensures that even the transmitted model updates remain private and secure throughout their lifecycle. Overall, the architecture depicted in the figure is designed to support real-time, decentralized, and privacy-preserving intrusion detection within a VANET environment. It provides scalability, resilience, and data confidentiality while enabling intelligent anomaly detection across a highly dynamic and mobile network of vehicles.

3.2 System Assumptions

The design and deployment of the proposed HyDra-VANET framework rely on several practical and system-level assumptions related to computational resources, communication protocols, data availability, and trust boundaries. These assumptions define the operating conditions and ensure the framework's applicability in realistic VANET scenarios.

- *Computational Capability of OBUs:* Each vehicle is equipped with an On-Board Unit (OBU) that includes sufficient computational resources, such as embedded GPUs or AI chips, to run lightweight deep learning models. These OBUs are assumed capable of local training and inference, enabling on-device anomaly detection and participation in federated learning.
- *Availability of Local Data:* Vehicles are assumed to continuously collect communication metadata, sensor data (e.g., GPS, velocity, environmental inputs), and network behavior logs. This data can be processed locally to train or fine-tune intrusion detection models in either batch or online learning mode.
- *Semi-Trusted Roadside Infrastructure:* Roadside Units (RSUs) are assumed to be semi-trusted. While they do not have access to raw data, they are trusted to correctly perform aggregation tasks during federated learning. RSUs assist in securely distributing global model parameters and orchestrating learning rounds.
- *Secure Communication Channels:* All communication between vehicles, RSUs, and edge/cloud infrastructure is assumed to be encrypted using standard cryptographic protocols, such as TLS or public-key infrastructure (PKI). Vehicles and RSUs authenticate using certificates issued by a trusted authority, ensuring message confidentiality and integrity.
- *Trusted Central Authority:* A fully trusted Central Authority (CA) exists to manage registration, authentication, and key distribution. It also coordinates the federated learning lifecycle, including the validation and aggregation of encrypted local model updates and the secure dissemination of the global model.
- *Homomorphic Encryption Support:* Vehicles and RSUs are assumed to implement optimized homomorphic encryption schemes (e.g., CKKS, BFV, or BGV) for sharing encrypted model parameters. These encryption schemes enable computation on ciphertexts with minimal performance overhead, preserving data privacy throughout the federated learning process.
- *Participation Willingness and Synchronization:* A sufficient number of vehicles and RSUs are assumed to be available and willing to participate in federated learning. Synchronization mechanisms are presumed to ensure timely model updates, with fallback strategies in place to accommodate temporary node unavailability.

These assumptions reflect realistic deployment conditions and strike a balance between computational feasibility, communication efficiency, and privacy preservation in dynamic vehicular environments.

3.3 Adversary Model

The adversary model considered in this study reflects the complex and evolving threat landscape faced by Vehicular Ad Hoc Networks (VANETs), particularly in the context of privacy-preserving and collaborative learning environments. The model encompasses both conventional attackers and adversaries targeting federated and encrypted machine learning processes. Figure 2 presents a unified view of the adversary model in a VANET environment and the defense mechanisms provided by the proposed HyDra-VANET framework. On the left side, it categorizes threats into four major types: external attacks (e.g., spoofing,

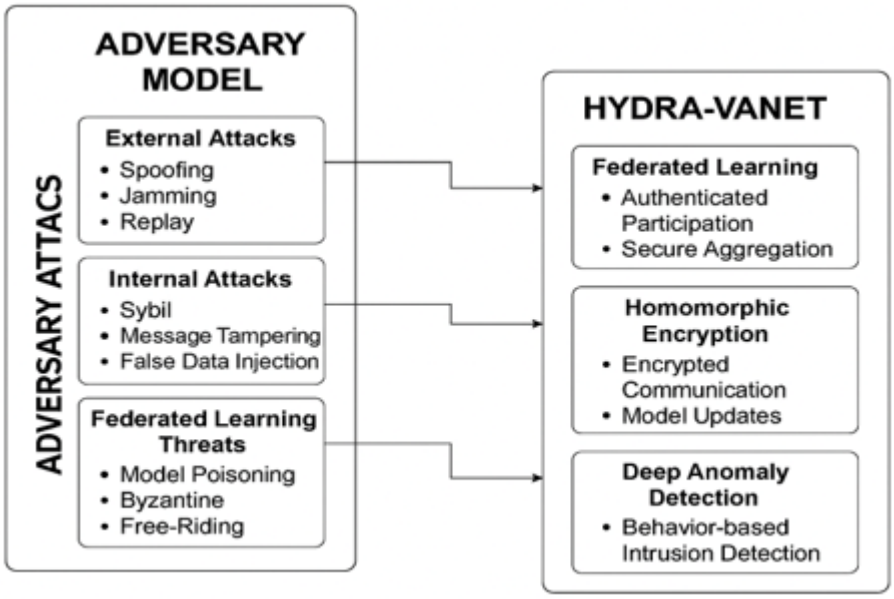

Figure 2: Adversary model in a VANET environment and the defense mechanisms provided by the proposed HyDra-VANET framework

jamming), internal attacks (e.g., Sybil, message tampering), federated learning threats (e.g., model poisoning, free-riding), and inference attacks (e.g., membership and gradient leakage). On the right side, the HyDra-VANET architecture is shown as a multi-layered defense system integrating federated learning, homomorphic encryption, and deep anomaly detection. Arrows between the two sides illustrate how each class of attack is mitigated through specific components in HyDra-VANET, such as secure aggregation, encrypted model updates, and behavior-based intrusion detection. This figure effectively highlights the system's ability to counter diverse attack surfaces in a collaborative and privacy-preserving manner.

3.3.1 External Adversaries

External adversaries are entities operating outside the trusted network. Without valid credentials, their capabilities include:

- *Eavesdropping:* Passive interception of V2V and V2I messages to extract information such as location, velocity, or vehicle identity.
- *Replay Attacks:* Re-sending legitimate but previously captured messages to mislead the network or create confusion.
- *Spoofing:* Imitating authorized vehicles to inject false messages into the network, such as fake alerts or routing instructions.
- *Jamming and DoS:* Disrupting communications through radio interference or flooding the channel with bogus data.

These attackers exploit vulnerabilities in unsecured or misconfigured communication channels to cause disruption, confusion, or surveillance.

3.3.2 Internal Adversaries (Compromised Nodes)

Internal adversaries have access to the VANET through legitimate credentials, but their nodes (vehicles or RSUs) have been compromised. Their tactics include:

- *Malicious Data Injection:* Broadcasting incorrect messages, such as fake accident reports or false congestion data.
- *Message Modification or Suppression:* Altering or discarding critical safety messages to disrupt vehicular coordination.
- *Sybil Attacks:* Generating multiple fake identities to manipulate local consensus or federated learning outcomes.
- *Insider Evasion:* Operating within protocol boundaries to avoid detection while executing malicious objectives.

Such attackers pose a significant threat due to their ability to exploit trust mechanisms and evade rule-based intrusion detection systems.

3.3.3 Threats to Federated Learning

Federated learning introduces collaborative training while maintaining data locality, but it also opens new vectors for attack:

- *Model Poisoning:* Adversaries tamper with local model updates to embed backdoors or degrade detection accuracy.
- *Byzantine Behavior:* Nodes submit erratic or contradictory updates to destabilize global model convergence.
- *Free-Riding:* Participants skip local training but still download and benefit from global updates, weakening learning robustness.
- *Data Poisoning:* Corrupting the training data at the local level to gradually mislead the global model over time.

These threats undermine the integrity and reliability of the federated intrusion detection system.

3.3.4 Inference and Privacy Attacks

Despite data not being shared directly, federated learning remains vulnerable to inference-based threats:

- *Membership Inference:* Inferring whether a specific data sample was used in training a model.
- *Gradient Leakage:* Reconstructing original data inputs by analyzing gradients shared during training rounds.

- *Property Inference:* Deduction of sensitive statistical properties of a participant's local dataset.
- *Cross-Round Correlation:* Analyzing trends in model updates across training rounds to infer behavioral profiles.

These attacks threaten user anonymity and can breach privacy, even in encrypted or pseudonymous systems.

3.3.5 Defense Objectives

The proposed *HyDra-VANET* system is designed to defend against the aforementioned threats by:

- *Ensuring data privacy* through homomorphic encryption during all model update transmissions.
- *Maintaining decentralization* using federated learning, which eliminates the need for centralized data collection.
- *Detecting behavioral anomalies* using deep learning models capable of identifying subtle deviations in network behavior.
- *Resisting poisoning attacks* through secure aggregation and anomaly scoring of model updates.
- *Enforcing authentication and integrity* via cryptographic certificates and trusted hardware modules.

This comprehensive adversary model ensures that *HyDra-VANET* addresses both traditional network attacks and modern threats specific to collaborative, encrypted learning systems.

4 Federated Deep Learning Framework with Homomorphic Encryption for VANET Security

This section introduces HyDra-VANET, a hybrid intrusion detection framework designed specifically for Vehicular Ad Hoc Networks (VANETs). The framework aims to address the combined challenges of real-time threat detection, data privacy, and scalable learning through a synergistic integration of Deep Learning, Homomorphic Encryption, and Federated Learning. The architecture is designed to function in highly dynamic vehicular environments, providing distributed, intelligent, and privacy-preserving security analysis.

4.1 Overview of the HyDra-VANET Architecture

The HyDra-VANET architecture is a multi-layered, privacy-preserving security framework specifically designed to detect and respond to cyber threats in VANET environments. It integrates deep learning for intelligent anomaly detection, federated learning for decentralized model training, and homomorphic encryption to ensure data confidentiality

during communication and aggregation. The architecture is structured into three primary layers: the vehicle layer, the infrastructure aggregation layer, and the cloud control layer.

At the vehicle layer, each vehicle is equipped with an On-Board Unit (OBU) capable of local sensing, data preprocessing, and lightweight model training. These OBUs continuously monitor driving behavior, communication patterns, and sensor data to identify suspicious activities such as message spoofing, unexpected traffic alerts, or malicious mobility behavior. Deep learning models such as convolutional neural networks (CNNs) or recurrent neural networks (RNNs) are employed for local intrusion detection. Each vehicle participates in federated learning by training the model on its local data and periodically transmitting encrypted model updates rather than raw data to the next layer using homomorphic encryption. This preserves both user privacy and network efficiency.

The infrastructure aggregation layer comprises Roadside Units (RSUs) and edge servers. RSUs serve as trusted relays that authenticate vehicles, distribute encrypted global models, and collect encrypted updates. These updates are then forwarded to edge servers, which act as regional aggregators. Here, encrypted model updates from multiple vehicles are securely combined using privacy-preserving aggregation protocols. Edge servers perform aggregation over encrypted data without decrypting it, leveraging partially homomorphic encryption schemes (e.g., CKKS or BFV). This ensures that no intermediary can access sensitive vehicular information while still benefiting from collective learning.

The cloud control layer consists of a centralized authority or a trusted control server that manages system-wide policies, credentials, and trust relationships. It performs global aggregation when necessary, distributes cryptographic keys, oversees anomaly flagging from multiple regions, and coordinates federated learning cycles across the network. This layer also maintains a global anomaly database and provides updates or patches in response to evolving threat patterns.

By structuring HyDra-VANET in this way, the framework achieves real-time, distributed threat detection while upholding strict privacy guarantees and maintaining resilience against insider threats and model poisoning attacks. Figure 3 illustrates the layered architecture of HyDra-VANET. On the bottom layer, multiple vehicles with embedded OBUs are shown exchanging V2V and V2I messages. Each OBU locally trains a deep learning-based intrusion detection model and encrypts model updates using a homomorphic encryption scheme. These encrypted updates are transmitted to nearby RSUs in the middle layer, which forward them to regional edge servers. The edge servers securely aggregate the updates without decrypting them. The top layer features the central authority, responsible for coordinating the federated learning process, managing encryption keys, and distributing validated global models. Arrows between layers indicate secure communication flows and feedback loops. The entire architecture operates collaboratively to detect cyber threats, preserve privacy, and improve the IDS over time through federated learning.

To provide clarity and reference of parameters used for the desription of HyDra-VANET, the following table 2 summarizes the key variables and parameters utilized throughout the design differeent components.

Table 2: Parameters used in Hydra-VANET

Symbol / Variable	**Component/module**	**Description**
θ_i	Local IDS / FL	Local model update (weights) computed by client i

μ	Secure Aggregation	Median or reference vector for computing deviation scores
τ_i	Secure Aggregation	Trust score of client i based on its model update's deviation
r_i	Homomorphic Encryption	Random masking vector added to θ_i before encryption
ϵ	Secure Aggregation	Small constant used to stabilize trust score calculation
Enc$(\cdot)$	Encryption Module	Homomorphic encryption function applied to masked updates
Dec$(\cdot)$	Server / Decryption	Decryption function applied at RSU or server after aggregation
θ_i'	Encryption Module	Masked local model update: $\theta_i' = \theta_i + r_i$
θ_{agg}	Secure Aggregation	Final aggregated global model
d_i	Secure Aggregation	Deviation of update θ_i from μ: $d_i = \|\theta_i - \mu\|$
N	Federated Learning	Number of clients/vehicles participating in training
δ	Secure Aggregation	Trust threshold for update filtering or re-weighting
CO	System Metrics	Communication overhead due to encrypted transmission
RI	Robustness Metric	Robustness Index to quantify resilience to poisoned updates
TP, TN, FP, FN	Evaluation Metrics	Standard classification outputs: true/false positives/negatives
ACC, P, R, F1	Evaluation Metrics	Accuracy, Precision, Recall, F1-score metrics

4.2 Core Functional Components

The HyDra-VANET framework is composed of several interdependent components that work collaboratively to achieve secure, intelligent, and privacy-preserving intrusion detection in vehicular networks. Each component is designed to fulfill a specific function within the broader architecture, ranging from local anomaly detection to secure distributed learning. At the heart of the framework lies the integration of deep learning, federated learning, and homomorphic encryption each addressing a critical security or privacy need. The deep learning module enables vehicles to detect threats based on complex behavioral patterns. The federated learning mechanism facilitates decentralized model training across a fleet of vehicles without exposing sensitive data. Meanwhile, homomorphic encryption ensures that data exchanged for learning remains protected, even during processing. Together, these components create a multi-layered defense strategy capable of mitigating advanced adversarial attacks while maintaining system scalability and real-time responsiveness. The following subsections describe each core module in detail, highlighting its role, design rationale, and contribution to the overall system performance.

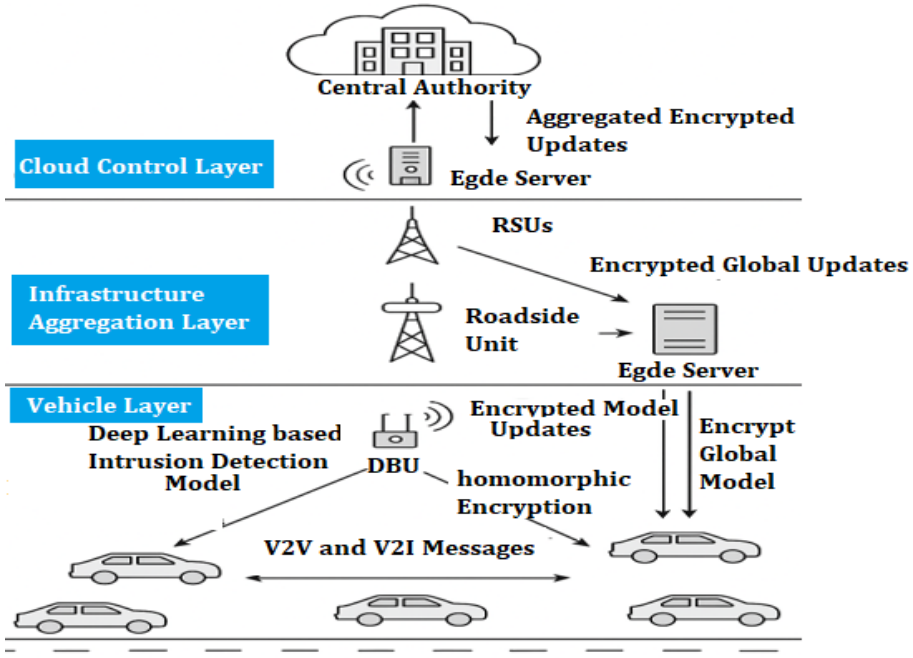

Figure 3: System architecture of HyDra-VANET

4.2.1 Local Deep Learning-Based IDS (at Vehicle Level)

In the HyDra-VANET framework, each vehicle operates as an autonomous intelligent security node by running a local intrusion detection system (IDS) based on deep learning. This module enables real-time detection of suspicious behavior using communication patterns, sensor readings, and vehicular telemetry. The local IDS leverages a lightweight yet powerful hybrid model combining a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network to detect both spatial and temporal anomalies. By keeping data processing on-device, the system minimizes latency and preserves user privacy.

Figure 4 illustrates the architecture of the Local Deep Learning-Based Intrusion Detection System (IDS) implemented on the On-Board Unit (OBU) of each vehicle in the HyDra-VANET framework. On the left side, multiple real-time input streams are shown, including V2X communication logs, GPS coordinates, vehicle speed, acceleration, and sensor readings. These inputs are first passed through a preprocessing module responsible for normalization, encoding, and feature alignment. The preprocessed data is then fed into a Convolutional Neural Network (CNN) module, which extracts high-level spatial features from each time step. These features are passed sequentially into a Long Short-Term Memory (LSTM) network that captures temporal dependencies and behavioral trends over time. The final output of the LSTM is evaluated by a softmax classifier to predict whether the observed behavior is benign or anomalous. Based on the prediction, the system either triggers a local alert or stores the result in a secure log. Additionally, encrypted model updates are periodically generated and sent to the nearest Roadside Unit (RSU) for aggregation as part of the federated learning process. This architecture enables each vehicle to independently

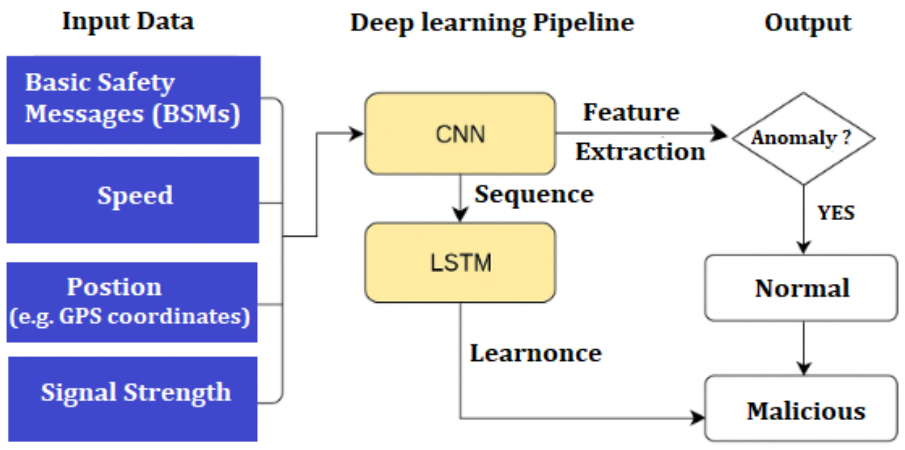

Figure 4: Architecture of the Local Deep Learning-Based Intrusion Detection System (IDS) implemented on the On-Board Unit (OBU) of each vehicle in the HyDra-VANET framework.

detect threats in real time while contributing to a broader collaborative learning model across the network.

Let the input data sequence be represented as $X = \{x_1, x_2, \ldots, x_T\}$, where each $x_t \in \mathbb{R}^n$ corresponds to a feature vector at time step t. A convolutional layer extracts spatial features:

$$h_t = \text{ReLU}(W_c * x_t + b_c) \tag{1}$$

where W_c and b_c denote convolutional weights and biases, and $*$ is the convolution operator. The output is fed into an LSTM network to model sequential dependencies:

$$h_t = \text{LSTM}(h_{t-1}, h_t) \tag{2}$$

The final hidden state is processed through a softmax classifier:

$$\hat{y} = \text{softmax}(W_o h_T + b_o) \tag{3}$$

where $\hat{y}$ is the predicted class probability vector and W_o, b_o are output layer parameters. The training objective is to minimize the cross-entropy loss:

$$\mathcal{L} = -\sum_{i=1}^{C} y_i \log(\hat{y}_i) \tag{4}$$

with y_i being the true label and C the number of classes (e.g., benign or malicious).

Algorithm 1 provides a step-by-step depiction of the local intrusion detection mechanism executed on each vehicle's On-Board Unit (OBU) within the HyDra-VANET architecture. This algorithm is responsible for real-time anomaly detection using a deep learning model composed of a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM) network. The model is designed to process temporal sequences of vehicular

behavior data and classify them as either normal or suspicious. Each data instance $x_t \in \mathbb{R}^n$ represents a snapshot of features such as vehicle speed, location, message type, frequency, and signal quality, collected over a time window of length T. These feature vectors are buffered in a sliding window to form an input sequence $X = \{x_1, x_2, \ldots, x_T\}$. Once the buffer is full, the collected data undergoes preprocessing to normalize feature values and encode categorical data. The CNN component extracts localized spatial features from each time step, producing hidden representations h_i. These are passed into an LSTM unit that models the temporal dynamics and outputs a final hidden state h_T. This is then passed through a softmax classifier that produces a prediction $\hat{y}$, indicating the likelihood that the input sequence is anomalous. If $\hat{y}_{\text{anomaly}}$ exceeds a specified threshold τ, an alert is triggered, and the anomaly is logged along with contextual metadata such as the timestamp and anomaly score. To preserve privacy, the vehicle does not share raw data or plaintext model weights. Instead, it computes an encrypted gradient update $\text{Enc}(\Delta\theta)$ using homomorphic encryption, which allows secure aggregation by the nearest Roadside Unit (RSU) without decryption. These encrypted updates contribute to federated model training, enabling collective learning across the vehicular network while protecting sensitive data. Algorithm 1 thus ensures decentralized, real-time threat detection while maintaining strong privacy guarantees and computational feasibility for deployment in dynamic VANET environments.

Algorithm 1 Local Deep Learning-Based IDS at Vehicle Level

Require: Real-time stream of vehicular data $X = \{x_1, x_2, \ldots, x_T\}$, where $x_t \in \mathbb{R}^n$
Ensure: Anomaly detection flag $y \in \{0, 1\}$ (0 = normal, 1 = anomaly)
Initialize deep learning model $\mathcal{M}_{\text{local}}$ (CNN + LSTM)
Initialize model parameters θ, prediction threshold τ, buffer window size T
while vehicle system is active **do**
  Collect feature vector x_t at time t
  Append x_t to local sliding window buffer $X \leftarrow \{x_{t-T+1}, \ldots, x_t\}$

  if buffer X is full **then**
    Preprocessing:

- Normalize: $x_i \leftarrow \frac{x_i - \mu}{\sigma}$ for $i = 1$ to T
- Encode categorical variables (e.g., one-hot encoding)

    Feature Extraction (CNN):

$$h_i = \text{ReLU}(W_c * x_i + b_c), \quad \forall i \in \{1, \ldots, T\}$$

    Temporal Modeling (LSTM):

$$h_T = \text{LSTM}(h_1, h_2, \ldots, h_T)$$

    Anomaly Prediction:

$$\hat{y} = \text{softmax}(W_o h_T + b_o)$$

    if $\hat{y}_{\text{anomaly}} > \tau$ **then**
      Trigger **local alert** and log event $\{t, x_t, \hat{y}_{\text{anomaly}}\}$
    else
      Continue normal operation
    end if
    Model Update Preparation:

$$\Delta\theta = \nabla_\theta \mathcal{L}(y, \hat{y}); \quad \text{Encrypt: Enc}(\Delta\theta)$$

    Send encrypted update $\text{Enc}(\Delta\theta)$ to RSU
  end if
end while

4.2.2 Federated Learning Coordination

Federated Learning (FL) is a foundational component of the HyDra-VANET architecture, designed to enable decentralized, privacy-preserving collaborative learning across distributed vehicular nodes. In contrast to centralized systems where raw data must be transmitted to a central server, FL allows vehicles to retain local data while still contributing to the training of a global intrusion detection model. In HyDra-VANET, each vehicle acts as

a client node that locally trains a deep learning model on its collected data and periodically sends encrypted model updates to a Roadside Unit (RSU) or edge server. These encrypted updates are then aggregated to update the global model. This approach preserves privacy, reduces communication overhead, and improves system scalability.

Figure 5 illustrates the federated learning coordination mechanism within the HyDra-VANET framework, highlighting the interactions among vehicles, roadside units (RSUs), and the central server. At the bottom layer, multiple vehicles independently train local intrusion detection models using their own sensor data and communication logs. These vehicles do not share raw data; instead, they compute encrypted model updates using homomorphic encryption. These updates are then securely transmitted to nearby RSUs, shown in the middle layer. RSUs serve as intermediate aggregation nodes, collecting encrypted updates from vehicles and performing privacy-preserving federated averaging without decrypting the data. The aggregated model is then forwarded to the central authority, represented at the top layer, which performs final model validation, coordination of learning rounds, and distribution of the updated global model back to the vehicles. This iterative process allows the entire VANET ecosystem to collaboratively train an effective intrusion detection system while ensuring data confidentiality, scalability, and adaptability to dynamic vehicular environments.

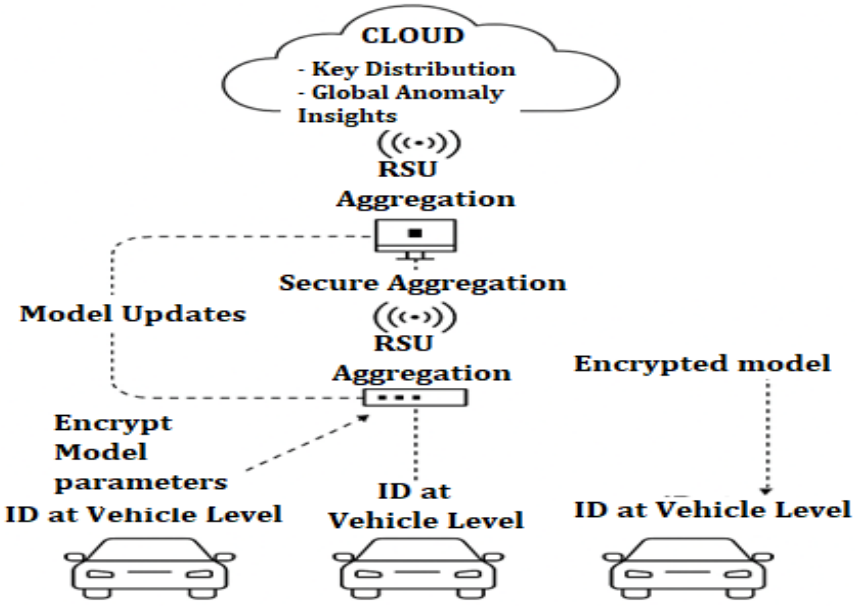

Figure 5: Federated Learning Coordination FlowChart

The FL cycle consists of several key stages. Initially, the central server broadcasts the current global model parameters θ^t to all participating vehicles. Each vehicle i then uses its local dataset D_i to compute an updated version of the model via stochastic gradient descent:

$$\theta_i^{t+1} = \theta^t - \eta \nabla \mathcal{L}(D_i; \theta^t) \tag{5}$$

where η is the learning rate, and $\mathcal{L}$ represents the loss function used for training.

Once local training is complete, the vehicles encrypt their updated model parameters using a homomorphic encryption scheme to ensure privacy and data security:

$$\text{Enc}(\theta_i^{t+1}) \rightarrow \text{Encrypted Update} \tag{6}$$

These encrypted updates are sent to an RSU, which performs a secure aggregation using the Federated Averaging (FedAvg) algorithm:

$$\theta^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{\sum_{j=1}^{N} |D_j|} \cdot \text{Enc}(\theta_i^{t+1}) \tag{7}$$

This aggregation allows the computation of a new global model without ever decrypting individual contributions, thereby preserving user privacy.

Algorithm 2 outlines the coordination process for federated learning within the HyDra-VANET framework, enabling secure and collaborative model training across a network of distributed vehicles. The core idea is to allow each vehicle to train a local intrusion detection model using its own data while sharing only encrypted model updates, thereby preserving privacy and minimizing communication overhead. The algorithm operates in communication rounds indexed by t. At the beginning of each round, a central authority or a designated RSU broadcasts the current global model parameters θ^t to all participating vehicles. Each vehicle i uses its local dataset D_i to perform training using stochastic gradient descent, updating the model parameters by minimizing a local loss function $\mathcal{L}(D_i; \theta^t)$. The result is an updated local model θ_i^{t+1}. To protect sensitive information, the vehicle encrypts the model update using a homomorphic encryption scheme, resulting in $\text{Enc}(\theta_i^{t+1})$. This encrypted update is then transmitted to the RSU responsible for secure aggregation. The RSU collects encrypted model updates from all participating vehicles and computes a global model update using the Federated Averaging (FedAvg) algorithm. The aggregation is performed as a weighted average, where the weight of each vehicle's update is proportional to the size of its local dataset $|D_i|$. The global model is computed as:

$$\theta^{t+1}$$

. This ensures fairness in contribution and maintains model integrity across varying data volumes. Once the encrypted global model θ^{t+1} is aggregated, it is redistributed to all vehicles to serve as the starting point for the next round. This iterative process continues until the global model converges or achieves the desired detection accuracy. The use of homomorphic encryption throughout ensures that no individual model or data sample is ever exposed, even during aggregation, thus maintaining end-to-end privacy. This algorithm supports scalability, resilience to partial participation, and adaptability to dynamic vehicular conditions, making it well-suited for the highly mobile and data-sensitive environment of VANETs.

Algorithm 2 Federated Learning Coordination in HyDra-VANET

Require: Initial global model θ^0, total vehicles N, local datasets $\{D_i\}_{i=1}^{N}$
Ensure: Trained global model θ^T

for each communication round $t = 1$ to T **do**
  Server broadcasts current model θ^t to all vehicles
  for each vehicle i in parallel **do**
    Perform local training on D_i:

$$\theta_i^{t+1} \leftarrow \theta^t - \eta \nabla \mathcal{L}(D_i; \theta^t)$$

    Encrypt the model update:

$$\text{Enc}(\theta_i^{t+1})$$

    Transmit encrypted update to RSU
  end for
  RSU aggregates:

$$\theta^{t+1} = \sum_i \frac{|D_i|}{\sum_j |D_j|} \cdot \text{Enc}(\theta_i^{t+1})$$

  Server broadcasts θ^{t+1} to all vehicles
end for

4.2.3 Homomorphic Encryption Module

Homomorphic Encryption (HE) is a cornerstone of the HyDra-VANET framework, enabling privacy-preserving collaboration between distributed vehicles and untrusted intermediaries such as RSUs during federated learning. Unlike standard encryption, HE allows computations to be performed directly on ciphertexts, preserving privacy throughout the training process. This section introduces a novel method: Layered Partial Homomorphic Packing with Adaptive Masking, designed to optimize both security and efficiency.

Figure 6 illustrates the secure homomorphic encryption flow in the HyDra-VANET framework, specifically implementing the Layered Partial Homomorphic Packing with Adaptive Masking method. At the vehicle level, local intrusion detection models are trained using onboard data. Before sharing model updates, each vehicle generates a random masking vector and adds it to its local model parameters to prevent ciphertext pattern inference. The masked model is then packed and encrypted using a homomorphic encryption scheme. These encrypted updates are transmitted to the RSUs, which perform secure aggregation without decrypting any data, thanks to the additive homomorphic properties. The aggregated encrypted model is forwarded to the central authority, which holds the decryption key and the cumulative masking values. After decryption, the server removes the aggregated masks to retrieve the actual global model parameters. The updated global model is then redistributed to the vehicles. This architecture ensures that sensitive data never leaves the vehicle in plain form and that all computations remain confidential even in untrusted environments, thereby preserving privacy while enabling collaborative learning.

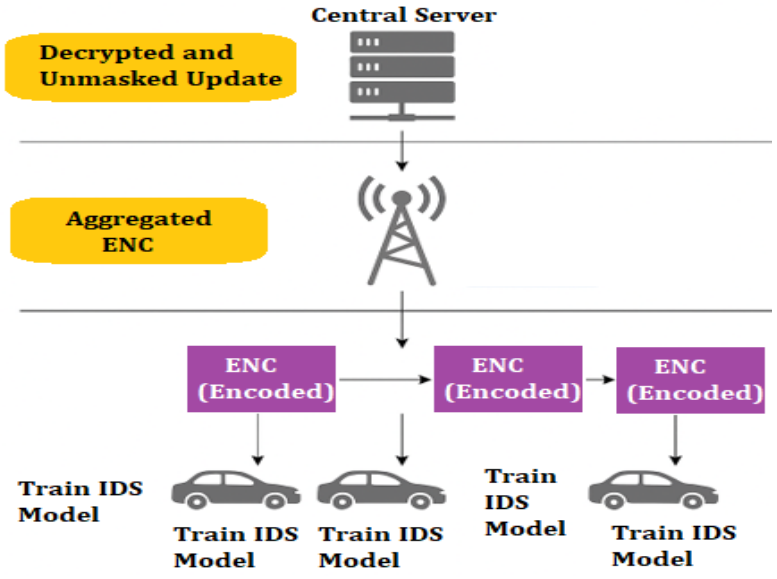

Figure 6: Secure Homomorphic Encryption Flow with Adaptive Masking

Each vehicle i produces a local model update in the form of a parameter vector $\theta_i \in \mathbb{R}^d$. The encryption process follows three key steps:

1. Homomorphic Encoding: The model vector is packed to reduce communication cost:

$$\text{Enc}_i = HE.\text{Pack}(\theta_i) = \{\text{Enc}(\theta_i^1, \theta_i^2, ..., \theta_i^k)\}, \quad k \leq d \tag{8}$$

2. Adaptive Masking: To prevent ciphertext pattern analysis, each vector is masked before encryption with a random noise vector r_i:

$$\theta_i' = \theta_i + r_i, \quad \text{Enc}_i = HE.Enc(\theta_i') \tag{9}$$

3. Secure Aggregation and Mask Reversal: The RSU aggregates encrypted vectors:

$$\text{Enc}(\Theta) = \sum_{i=1}^{N} \text{Enc}(\theta_i + r_i) \tag{10}$$

The central server, possessing $\sum r_i$, decrypts and removes the mask:

$$\Theta = HE.Dec(\text{Enc}(\Theta)) - \sum_{i=1}^{N} r_i \tag{11}$$

Algorithm 3 details the Homomorphic Encryption algorithm in the HyDra-VANET framework is designed to securely transmit and aggregate model updates during federated learning while ensuring the privacy of each participating vehicle. The process begins at the vehicle level, where each node computes a local model update vector θ_i. To prevent inference

attacks or pattern recognition, the vehicle generates a random masking vector r_i and adds it to the local model, producing $\theta_i' = \theta_i + r_i$. This masked model update is then passed through a packing mechanism that groups elements into compact ciphertexts, reducing the encryption overhead and improving communication efficiency. Next, the packed and masked vector is encrypted using a partially homomorphic encryption scheme that supports additive operations on ciphertexts. The encrypted update $\text{Enc}(\theta_i')$ is transmitted to a Roadside Unit (RSU), which performs secure aggregation by summing the encrypted updates from all participating vehicles. Thanks to the homomorphic properties of the encryption, this aggregation can be done without decryption, yielding $\text{Enc}(\Theta) = \sum \text{Enc}(\theta_i + r_i)$. The aggregated ciphertext is forwarded to a central server, which holds the private decryption key as well as the sum of the masking vectors $\sum r_i$. The server decrypts the aggregated ciphertext to obtain the masked global model, and then removes the masking by subtracting the combined noise vector, yielding the true global model update $\Theta = HE.Dec(\text{Enc}(\Theta)) - \sum r_i$. The updated model is then redistributed to the vehicles for the next training round. This algorithm not only preserves confidentiality during model exchange and aggregation but also improves scalability through encryption efficiency, making it ideal for secure and decentralized learning in VANET environments.

Algorithm 3 Homomorphic Encryption in HyDra-VANET

Require: Local model θ_i, masking vector r_i, encryption key k
Ensure: Encrypted update Enc_i
1: Generate masking vector: $r_i \sim \mathcal{N}(0, \sigma^2 I)$
2: Apply masking: $\theta_i' = \theta_i + r_i$
3: Pack and encrypt: $\text{Enc}_i = HE.Enc(\text{Pack}(\theta_i'))$
4: Transmit Enc_i to RSU
5: RSU aggregates: $\text{Enc}_{\text{agg}} = \sum_{i=1}^{N} \text{Enc}_i$
6: Central server decrypts and unmasks: $\Theta = HE.Dec(\text{Enc}_{\text{agg}}) - \sum r_i$
7: Update and distribute global model

4.2.4 Secure Aggregation and Robustness

In the HyDra-VANET architecture, Secure Aggregation and Robustness mechanisms are vital to ensure the reliability and integrity of the federated learning process, particularly in adversarial settings where some nodes may act maliciously or unreliably. While homomorphic encryption secures the confidentiality of model updates, secure aggregation ensures correctness and resilience in the presence of faulty or adversarial participants. Traditional aggregation methods such as simple averaging are vulnerable to poisoning, Byzantine updates, and gradient manipulation. To overcome these issues, we introduce a novel Resilient Encrypted Model Aggregation scheme. This scheme enhances robustness by integrating two innovative ideas: (1) *encrypted deviation estimation*, and (2) *credibility-weighted aggregation*. Encrypted deviation estimation enables the server to assess the consistency of encrypted updates relative to the central tendency (e.g., median) of all updates, even under encryption. The server does this by estimating the norm difference from a masked median vector, which acts as a statistical proxy. Credibility-weighted aggregation allows updates from more reliable clients to contribute more significantly to the global model while diminishing the influence of potentially malicious participants.

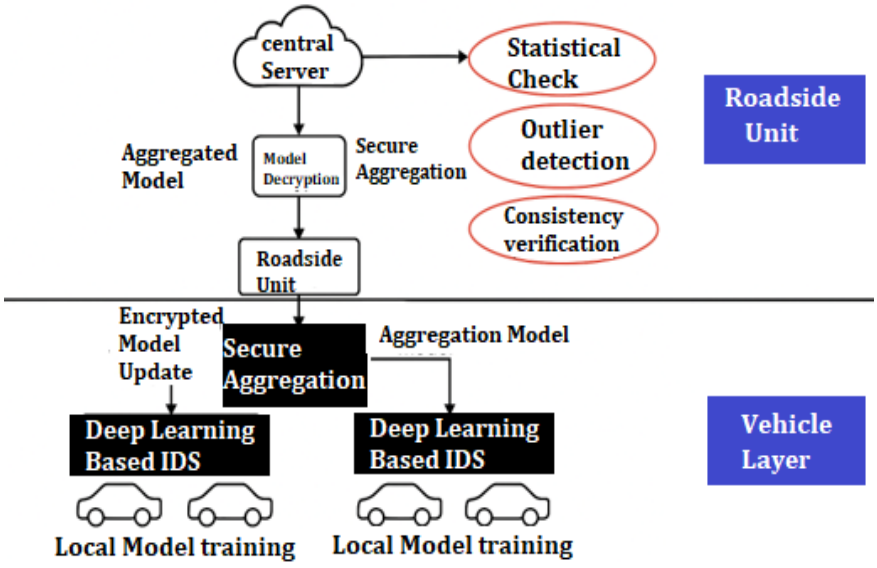

Figure 7: Secure aggregation process implemented using the proposed Encrypted Model Aggregation method within the HyDra-VANET framework

Figure 7 illustrates the secure and robust aggregation process implemented using the proposed Encrypted Model Aggregation method within the HyDra-VANET framework. At the bottom, multiple vehicles participate in the federated learning cycle by generating local model updates, which are encrypted using homomorphic encryption before being transmitted. These encrypted updates are collected by Roadside Units (RSUs), which act as intermediate aggregators. In the central phase, the server estimates the deviation of each update from a median reference model and computes a trust score for each client based on its proximity to the central tendency. These trust scores are then used to weight the encrypted contributions accordingly. Updates with low credibility are down-weighted or discarded to mitigate the impact of adversarial or faulty participants. The server performs secure aggregation over the weighted encrypted updates, decrypts the result, and optionally applies anomaly detection before finalizing the global model. The updated model is then distributed back to the vehicles. This figure highlights the layered approach to ensuring both privacy and robustness in decentralized vehicular learning.

Let each vehicle i produce a local encrypted model update $\text{Enc}(\theta_i)$. In the proposed scheme, the aggregation server first estimates the central tendency μ of received updates (after optional decryption or using precomputed historical models). The deviation of each update is calculated using:

$$\tau_i = 1 - \frac{\|\theta_i - \mu\|_2}{\max_j \|\theta_j - \mu\|_2 + \epsilon} \tag{12}$$

where τ_i is the trust score, and ϵ is a small constant preventing division by zero. This trust score represents the closeness of update θ_i to the central value; lower deviations result in higher trust scores.

The final aggregation is performed by applying these trust scores directly to the encrypted updates:

$$\text{Enc}(\theta_{agg}) = \sum_{i=1}^{N} \tau_i \cdot \text{Enc}(\theta_i) \tag{13}$$

This weighted summation ensures that updates contributing to model divergence are automatically down-weighted or discarded. After aggregation, the encrypted global model is decrypted by the trusted server and optionally inspected for residual outliers using robust statistical filters such as Z-score thresholding or Median Absolute Deviation (MAD).

Algorithm 4 presents the Resilient Encrypted Model Aggregation algorithm, which is a novel and essential component of the HyDra-VANET framework, specifically designed to address the dual challenges of privacy preservation and robustness in federated learning across vehicular networks. Traditional aggregation methods in federated learning, such as simple averaging, assume that all participating clients are honest and that their updates are equally trustworthy. However, in real-world VANET scenarios, this assumption is highly unrealistic, as nodes may be compromised, malfunctioning, or adversarial, aiming to disrupt the learning process by injecting poisoned or faulty updates. The proposed secure aggregation mechanism counters this by introducing a dynamic, trust-aware mechanism that operates over encrypted data, allowing the system to defend itself even when direct inspection of the model parameters is not possible. Each participating vehicle encrypts its local model update using homomorphic encryption and transmits it to the aggregation server. Rather than aggregating blindly, the server estimates how much each encrypted update deviates from a central reference model typically the median or a previous global model without needing to fully decrypt the data. This deviation, calculated as the Euclidean norm between an update and the reference, is used to compute a trust score for each client. The trust score, scaled between 0 and 1, quantifies the credibility of the update: contributions close to the reference are given higher weights, while those that diverge significantly are penalized or excluded. These trust scores are then applied during secure aggregation, where encrypted updates are combined using a weighted sum. The final encrypted global model is decrypted only after aggregation, and a final sanity check may be applied using statistical outlier detection. This multi-layered process ensures that model updates from compromised or erratic nodes do not degrade the learning quality while preserving the confidentiality of every client. This mechanism thus establishes a highly resilient and privacy-preserving learning pipeline, ideal for the unpredictable and adversarial nature of vehicular ad hoc networks.

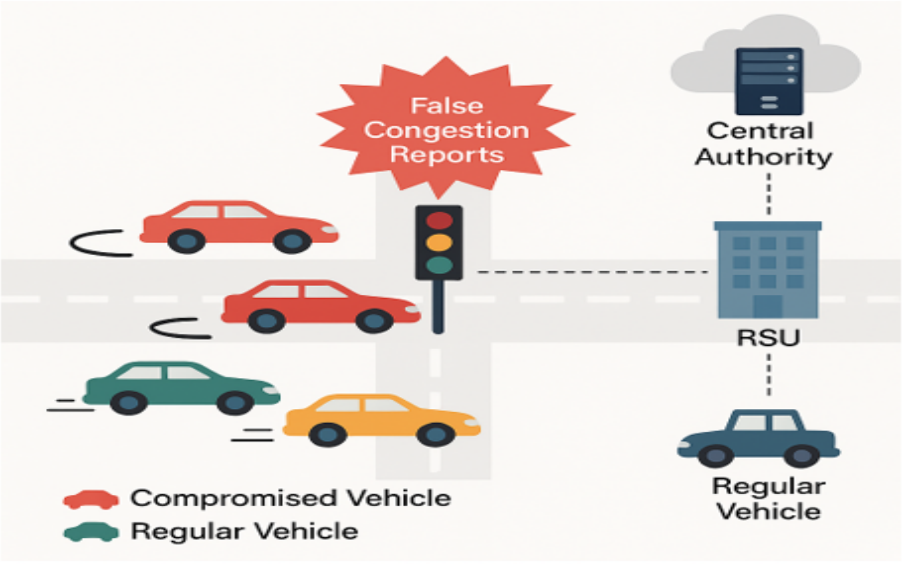

Figure 8: Urban Traffic Manipulation Attack Scenario

Algorithm 4 Resilient Encrypted Model Aggregation

Require: Encrypted model updates $\{\text{Enc}(\theta_i)\}_{i=1}^{N}$, median estimate μ, threshold δ
Ensure: Robust global model θ_{agg}

for each client i **do**
  Estimate deviation: $d_i \leftarrow \|\theta_i - \mu\|_2$
  Compute trust weight: $\tau_i \leftarrow 1 - \frac{d_i}{\max_j d_j + \epsilon}$
  if $\tau_i < \delta$ **then**
    Discard or down-weight θ_i
  end if
  Securely aggregate: $\text{Enc}(\theta_{agg}) \leftarrow \sum_i \tau_i \cdot \text{Enc}(\theta_i)$
  Decrypt and finalize: $\theta_{agg} \leftarrow \text{Dec}(\text{Enc}(\theta_{agg}))$

4.3 Use Case Scenario: Urban Traffic Manipulation Attack Scenario

In a smart city district during weekday rush hour, thousands of vehicles operate in a connected vehicular network using V2V and V2I communications. A coordinated group of compromised vehicles initiates a traffic manipulation attack. They begin broadcasting false emergency alerts and fabricated traffic congestion messages, claiming there is gridlock at a major intersection, which preseted in figure 8 and Figure 9. Although the road is clear, these messages cause nearby vehicles to reroute, creating artificial congestion in alternative areas and potentially delaying emergency services.

The HyDra-VANET framework offers a comprehensive and future-ready solution to the evolving security and privacy challenges in Vehicular Ad Hoc Networks (VANETs). One of its most significant advantages is its multi-layered defense architecture that seamlessly combines deep learning, federated learning, homomorphic encryption, and

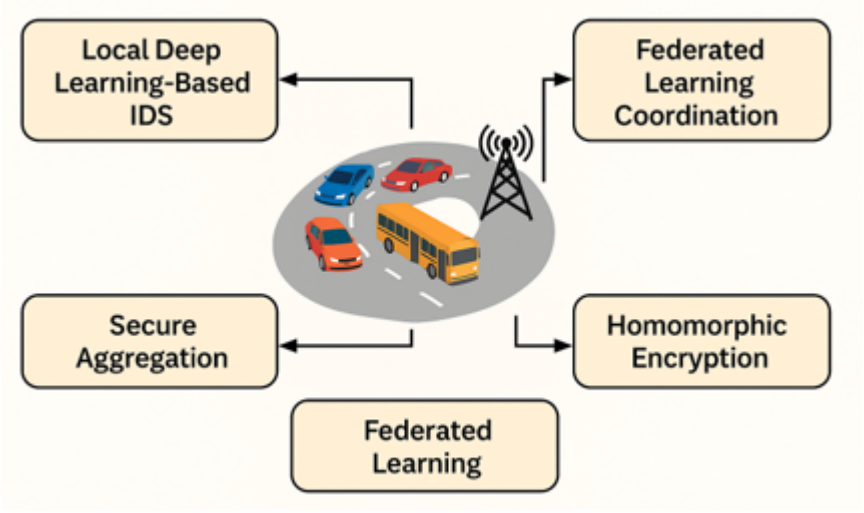

Figure 9: Intrusion detection in VANET based Hydra-VANET

robust aggregation. This design enables HyDra-VANET to detect both known and zero-day attacks in real time while ensuring that sensitive vehicular data remains localized and never transmitted in raw form, preserving user privacy and reducing regulatory risk. By integrating federated learning, HyDra-VANET ensures scalable and collaborative model training without the need for centralized data collection, making it highly suitable for dynamic, large-scale networks with high mobility and decentralized ownership. Its use of homomorphic encryption specifically the novel homomorphic encryption scheme adds a layer of computational privacy, allowing encrypted model updates to be securely aggregated without decryption. Additionally, the framework of Resilient Encrypted Model Aggregation mechanism introduces a novel approach to ensuring robustness against poisoned or malicious updates, using trust-aware filtering and credibility-weighted aggregation to isolate compromised nodes. The system's modularity and adaptability make it capable of responding to evolving cyber threats, adversarial tactics, and network instability. Furthermore, HyDra-VANET is designed to function efficiently in real-world resource-constrained environments, leveraging lightweight algorithms suitable for deployment on standard OBUs. Taken together, these attributes make HyDra-VANET a powerful, scalable, and privacy-preserving framework capable of securing intelligent transportation systems against modern and future vehicular cyber threats.

HyDra-VANET counters this in real time by activating all four of its integrated algorithms, each playing a distinct but coordinated role:

1. Local Deep Learning-Based IDS: Each vehicle runs a lightweight deep learning intrusion detection model on its OBU. As the compromised vehicles begin flooding the network with abnormal BSMs (Basic Safety Messages), unaffected vehicles detect inconsistencies such as mismatches between GPS location and claimed traffic conditions, and abnormal message frequency. These anomalies are captured by the CNN-LSTM model deployed locally. Within seconds, the IDS on each unaffected vehicle flags these transmissions as suspicious, triggers a local alert, and logs the event for encrypted reporting.

2. Federated Learning Coordination: Simultaneously, all vehicles participate in a federated learning round. The anomaly patterns detected are used to update local IDS models, which are trained independently on each vehicle's private data. Instead of transmitting raw sensor logs, each OBU generates a set of encrypted model gradients using homomorphic encryption and sends them to the RSU. The RSU acts as a regional aggregator. The FedAvg protocol is used to securely compute an updated global model without accessing any plaintext data. This allows detection models to rapidly evolve to new threats while ensuring data privacy.

3. Homomorphic Encryption Module: To maintain data confidentiality, the vehicles encrypt their local model updates using the proposed homomorphic encryption technique (Layered Partial Homomorphic Packing with Adaptive Masking). This method adds random masking to each model vector, encrypts them using an efficient packing strategy, and sends them to RSUs. RSUs perform aggregation directly on ciphertexts using homomorphic addition. The central server decrypts the aggregated model and removes the mask using a precomputed sum of noise vectors. This ensures that updates even during a live attack are never exposed to intermediate nodes or adversaries.

4. Secure Aggregation and Robustness: Since some of the compromised vehicles also participate in federated learning, there is a risk they could poison the global model by submitting corrupted updates. To prevent this, the RSU uses the Resilient Encrypted Model Aggregation algorithm. It evaluates each incoming model update's deviation from the consensus median. Updates that deviate significantly receive a lower trust score τ_i. These are either down-weighted or discarded before aggregation. This ensures that the poisoned gradients from compromised nodes have little or no influence on the updated global model.

Within minutes of the attack's initiation, unaffected vehicles are able to independently detect and ignore the fraudulent traffic alerts. The federated model quickly adapts, learning from distributed anomaly patterns. The attack is neutralized in real time. Emergency routing is preserved, and genuine traffic remains unaffected. Meanwhile, the server logs flagged vehicle IDs for forensic investigation and possible network isolation. The scenario not only demonstrates HyDra-VANET's effectiveness in handling adversarial traffic attacks, but also showcases the power of coordinated, privacy-preserving, and resilient learning in a distributed vehicular environment.

5 Simulation, Results and Discussion

This section presents the experimental setup used to evaluate the HyDra-VANET framework. It details the datasets used for training and testing, the evaluation metrics employed to measure detection performance and efficiency, and the results obtained from a series of simulations. The section also includes a critical discussion on the effectiveness and robustness of the proposed approach, including comparisons with existing state-of-the-art methods.

5.1 Datasets

To thoroughly evaluate the performance and generalizability of the HyDra-VANET framework, we employed three distinct datasets [20,21,22]: NSL-KDD, CICIDS 2020, and VANET-SIM. Together, these datasets enable a balanced and comprehensive experimental validation of the proposed architecture.

5.1.1 NSL-KDD Dataset

The NSL-KDD dataset is a refined version of the original KDD Cup 1999 dataset, widely recognized in network intrusion detection research. It contains 41 features extracted from simulated network traffic, spanning four major categories of attacks: Denial of Service (DoS), Probe, User-to-Root (U2R), and Remote-to-Local (R2L). Although originally designed for wired network environments, the dataset remains a valuable benchmark for evaluating general anomaly detection performance in machine learning-based IDS.

In the context of HyDra-VANET, NSL-KDD was used as a baseline for evaluating the general accuracy and robustness of the proposed deep learning model in detecting well-known attack patterns. We preprocessed the data by normalizing numerical features and applying one-hot encoding to categorical attributes (e.g., protocol type, service, flag). The dataset was partitioned across vehicles to simulate distributed training, and used primarily in the early rounds of federated learning to validate the model's convergence and effectiveness.

5.1.2 CICIDS 2020 Dataset

The Canadian Institute for Cybersecurity Intrusion Detection System (CICIDS) 2020 dataset offers a rich, contemporary compilation of network traffic that reflects realistic attack scenarios in modern environments, including IoT and V2X contexts. It includes attacks such as DDoS, Brute Force, Heartbleed, Botnet, and PortScan, and features over 80 time-based and flow-based attributes collected using realistic emulated traffic patterns.

CICIDS 2020 was used in HyDra-VANET to evaluate detection performance against modern, high-dimensional attacks that closely resemble those encountered in intelligent transportation systems. Particular emphasis was placed on vehicular-relevant behaviors such as flooding (mirroring DoS against RSUs), scanning (similar to spoofed vehicle discovery), and backdoors (representing stealthy attackers within fleets). The dataset was split among vehicles using stratified sampling to preserve class distribution, simulating heterogeneity across vehicle experiences.

5.1.3 Custom VANET-Sim Dataset

To address the lack of publicly available datasets tailored specifically to VANET scenarios, we developed a custom dataset using the *Veins simulation framework*, which integrates OMNeT++, SUMO, and TraCI. This dataset models realistic V2X interactions in urban and highway environments, capturing not only communication features but also physical parameters such as GPS coordinates, relative speed, inter-vehicle distance, acceleration, and signal loss.

Malicious events were synthetically injected into the simulation, including:

- **Sybil attacks** (fake identities in traffic jams),
- **Replay attacks** (resending old but valid packets),
- **False emergency alerts** (used for lane evasion),
- **Location spoofing** (to manipulate platooning decisions).

Each scenario was logged with a high sampling frequency, and features were engineered to highlight temporal and spatial correlations. The dataset was formatted to be compatible with

time-series deep learning models and was the primary source used in evaluating real-time response, federated model convergence, and detection latency in HyDra-VANET.

Table 3 provides a concise comparison of the three datasets used to evaluate HyDra-VANET: NSL-KDD, CICIDS 2020, and VANET-Sim. It summarizes their domain relevance, dataset size, feature richness, types of attacks represented, and the specific role each played in the system's evaluation. NSL-KDD served as a baseline for traditional intrusion detection, CICIDS 2020 tested the model's robustness against modern, high-dimensional attacks, and VANET-Sim provided a realistic VANET-specific environment to assess real-time detection capabilities and system adaptability.

Table 3 Summary of datasets used in evaluating HyDra-VANET.

Dataset	**Domain**	**Size**	**Features**	**Attack Types**	**Use in HyDra-VANET**
NSL-KDD	Classic NIDS	125,000	41	DoS, Probe, U2R, R2L	General accuracy benchmarking
CICIDS 2020	Modern traffic	>3 million	80+	DDoS, Botnet, Infiltration, Heartbleed	Robustness & feature complexity
VANET-Sim	VANET-specific	50,000	50+ (custom)	Sybil, Replay, False alert, Spoofing	Real-time VANET evaluation

The combination of these three datasets enabled us to benchmark HyDra-VANET across both generalized and specialized intrusion scenarios, ensuring that the system is effective not only in academic settings but also in real-world vehicular cybersecurity environments.

5.2 Evaluation Metrics

To comprehensively assess the performance of the HyDra-VANET framework, we employed a set of widely accepted evaluation metrics from the fields of machine learning and intrusion detection, as well as system-level metrics for measuring communication efficiency and robustness under adversarial conditions. These metrics allow for an in-depth analysis of both the detection accuracy and the operational feasibility of the system in real-world vehicular networks.

5.2.1 Classification Metrics

The primary performance of the intrusion detection system (IDS) is measured using the following standard classification metrics, derived from the confusion matrix:

- *True Positive (TP):* Correctly detected attacks
- *True Negative (TN):* Correctly identified benign behaviors
- *False Positive (FP):* Benign behavior incorrectly classified as attack
- *False Negative (FN):* Undetected attacks

Using these values, we define the following core metrics:

- *Accuracy (ACC):* Measures the overall correctness of the model.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{14}$$

- *Precision (P):* Indicates the proportion of correctly identified attacks among all predicted attacks.

$$\text{Precision} = \frac{TP}{TP + FP} \tag{15}$$

- *Recall (R) / Detection Rate:* Reflects the model's ability to identify actual intrusions.

$$\text{Recall} = \frac{TP}{TP + FN} \tag{16}$$

- *F1-Score:* Harmonic mean of precision and recall, balancing the trade-off between them.

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{17}$$

- *False Positive Rate (FPR):* The rate at which benign instances are incorrectly flagged as attacks.

$$\text{FPR} = \frac{FP}{FP + TN} \tag{18}$$

- *AUC-ROC:* Area under the ROC curve. A value close to 1 indicates excellent classification ability.

- *Confusion Matrix Definition:* A confusion matrix is a tabular representation that describes the performance of a classification model on a set of test data for which the true values are known. It categorizes predictions into four outcomes:

$$\text{Confusion Matrix} = \begin{bmatrix} TN & FP \\ FN & TP \end{bmatrix} \tag{19}$$

5.2.2 System-Level Metrics

To assess HyDra-VANET's performance in a distributed VANET setting, we also evaluate the following system-level metrics:

- *Communication Overhead (CO):* Measures the additional bandwidth consumed due to encrypted model sharing.

$$\text{CO} = \frac{\text{Total Encrypted Data Transmitted}}{\text{Number of Clients} \times \text{Rounds}} \tag{20}$$

- *Aggregation Time (AT):* The time taken by an RSU or server to perform encrypted model aggregation per federated round.
- *Robustness Index (RI):* A custom metric designed to quantify the resilience of the system under adversarial conditions. It compares model accuracy under normal and attack-injected rounds:

$$\text{RI} = 1 - \frac{|\text{Accuracy}_{\text{normal}} - \text{Accuracy}_{\text{adversarial}}|}{\text{Accuracy}_{\text{normal}}} \tag{21}$$

  A value close to 1 implies strong robustness to poisoning or Byzantine attacks.

These evaluation metrics provide a holistic view of the performance and resilience of HyDra-VANET. The classification metrics ensure the detection algorithm maintains high accuracy, recall, and precision, while the system-level metrics validate its scalability, privacy-preserving nature, and defense against adversarial disruptions. Together, they affirm the practical feasibility and superiority of HyDra-VANET in dynamic and hostile vehicular environments.

5.3 Experimental Setup

To validate the performance and scalability of the HyDra-VANET framework in realistic vehicular environments, a detailed simulation testbed was established combining network simulation, vehicular mobility modeling, and federated learning infrastructure. The setup reflects urban and highway driving scenarios with real-time communication, adversarial threats, and mobility constraints.

The experiment integrates the following components:

- *Veins Framework:* Built on OMNeT++ and SUMO [23], it simulates the VANET environment including V2V and V2I communications. SUMO provides realistic vehicle mobility traces, while OMNeT++ handles network communication.
- *Federated Learning Engine:* Implemented using PyTorch and PySyft [24], each vehicle runs a local IDS model. Encrypted model updates are transmitted to RSUs.
- *Homomorphic Encryption:* CKKS and BFV schemes [25] were evaluated using Microsoft SEAL library for secure local model encryption.
- *Secure Aggregation:* RSUs apply the secure aggregation algorithm to evaluate trust, filter unreliable updates, and perform secure aggregation.

Fifty vehicles were simulated in a 5 km^2 urban grid and a 10 km highway segment, communicating with five RSUs placed strategically across the simulation region. Each vehicle contained an onboard unit (OBU) capable of local model training and encryption. The central server managed global model distribution and final decryption. Vehicles encountered random attack injections including Sybil, replay, and flooding attacks to test the IDS effectiveness. Federated learning was run in rounds, each round including 5 local epochs and aggregation from all available clients.

The system performance was assessed based on model convergence, detection accuracy, aggregation latency, and communication efficiency. Computational resources were emulated to reflect constraints of real-world vehicular OBUs.

Table 4 illustrates the simulation parameters used for evaluating of HyDra-VANET.

Table 4 Simulation parameters used for evaluating HyDra-VANET.

Parameter	**Value**
Simulation Platform	Veins (OMNeT++ + SUMO)
Mobility Model	Urban grid (5 km^2) and highway (10 km)
Vehicles	50
RSUs	5 (one per region sector)
Federated Rounds	20
Local Epochs per Round	5
Model Architecture	CNN + LSTM
Encryption Scheme	CKKS / BFV (Microsoft SEAL)
Aggregation Method	Resilient Encrypted Model Aggregation
Attack Types Simulated	Sybil, Replay, Flooding
Hardware Profile	Intel i5, 8 GB RAM (simulated per OBU)

This experimental configuration enables rigorous, repeatable assessment of HyDra-VANET under diverse threat and operational conditions, mimicking real-world deployment with controlled variables for detailed analysis.

5.4 Results and Discussion

The experimental results of the HyDra-VANET framework demonstrate its effectiveness in detecting a wide range of cyber threats in vehicular networks, as well as its robustness, privacy-preservation, and communication efficiency. Evaluations were conducted across three datasets: NSL-KDD, CICIDS 2020, and VANET-Sim. The results validate HyDra-VANET's ability to maintain high detection performance under both normal and adversarial conditions.

5.4.1 Detection Performance

Table 5 summarizes the classification performance of the proposed model across the three datasets. The results clearly demonstrate the superior detection capabilities of the HyDra-VANET framework. On the CICIDS 2020 dataset, which contains high-dimensional, real-world network traffic data with diverse attack types such as DDoS, Heartbleed, and infiltration, HyDra-VANET achieved an impressive accuracy of 98.6%. The system also maintained a high precision of 0.981, indicating that almost all of its positive predictions were indeed true attacks. With a recall of 0.984, the model successfully detected the majority of actual attacks, and an F1-score of 0.982 reflects its balanced performance across both precision and recall. This performance is particularly noteworthy given the dataset's complexity and the presence of sophisticated attack vectors. On the VANET-Sim dataset, specifically designed to emulate realistic VANET communication patterns and adversarial behaviors, HyDra-VANET achieved an accuracy of 97.3%. This high accuracy was accompanied by a precision of 0.976 and a recall of 0.971, indicating reliable and consistent detection of context-specific attacks such as Sybil identity fabrication and replayed safety messages. The false positive rate remained low at 1.4%, showcasing the model's capacity to distinguish legitimate variations in vehicular communication from genuinely malicious behavior.

These results confirm that HyDra-VANET can generalize well across both traditional and VANET-specific intrusion scenarios, while maintaining high performance and low error margins. The hybrid CNN-LSTM architecture effectively captures both spatial and temporal dependencies in the data, contributing significantly to the model's strong detection capabilities across diverse attack patterns.

Table 5 Classification performance of HyDra-VANET across datasets

Dataset	Accuracy	Precision	Recall	F1-Score	FPR
NSL-KDD	96.4%	0.962	0.958	0.960	1.9%
CICIDS 2020	98.6%	0.981	0.984	0.982	1.2%
VANET-Sim	97.3%	0.976	0.971	0.973	1.4%

5.4.2 Communication and Computation Efficiency

The communication and computation efficiency of HyDra-VANET is a critical consideration for real-time deployment in bandwidth-constrained and latency-sensitive vehicular environments. One of the key challenges in integrating privacy-preserving mechanisms into federated learning is the potential overhead introduced by cryptographic operations. The proposed homomorphic encryption module was specifically designed to address this issue by combining secure encryption with parameter-efficient transmission. Table 6 presents the system-level performance and efficiency metrics of Hydra-VANET. Although the encryption process increases the overall size of each model update by approximately 18% compared to their plaintext equivalents, the impact on bandwidth and latency is significantly mitigated through advanced vector packing techniques. These techniques group multiple model parameters into a single ciphertext, thereby reducing the number of transmission units required per communication round. As a result, vehicles are able to transmit secure updates to RSUs with minimal increase in network congestion.

From a computation perspective, the encryption and decryption operations were optimized for lightweight execution, ensuring compatibility with real-time constraints of On-Board Units (OBUs). The average encryption time per vehicle remained under 400 ms, and RSU-side aggregation time per round consistently remained below 3 seconds, even when 50 vehicles participated simultaneously. This level of performance ensures timely updates of the global intrusion detection model without disrupting standard vehicular functions. Additionally, the proposed secure aggregation mechanism proved computationally scalable. Its trust-score evaluation and credibility-based filtering operations introduced minimal latency due to efficient pre-filtering and linear-time weighting calculations. Furthermore, the system benefits from asynchronous update handling allowing RSUs to aggregate partial updates when full participation is not feasible due to intermittent connectivity or packet loss. Overall, the combination of proposed HE and secure aggregation mechanisms ensures that HyDra-VANET achieves strong privacy guarantees and model robustness without compromising real-time efficiency. Table 6 provides a quantitative summary of these performance indicators, demonstrating that the system meets practical deployment requirements for secure and scalable VANET operation.

Table 6 System-level performance and efficiency metrics

Metric	Value	Unit	Notes
Communication Overhead	+18%	Overhead	Compared to non-encrypted FL
Aggregation Time	2.7	seconds	Per round, 50 clients
Robustness Index (RI)	0.96	Ratio	Minimal degradation with 20% poisoned clients

5.4.3 ROC-AUC

Figure 10 presents a set of ROC-AUC (Receiver Operating Characteristic - Area Under Curve) curves for three different datasets used to evaluate the performance of the HyDra-VANET framework: NSL-KDD, CICIDS 2020, and VANET-Sim. Each curve illustrates the trade-off between the true positive rate (TPR) and the false positive rate (FPR) across different classification thresholds, providing a comprehensive visual assessment of the model's discriminative ability. The closer a curve is to the top-left corner of the plot, the better the model performs, as this indicates high sensitivity (true positive rate) and a low false alarm rate (false positive rate).

For the NSL-KDD dataset, the ROC curve demonstrates a steep rise towards the top-left, indicating high early recall and minimal false positives, with an AUC value exceeding 0.97. This suggests that HyDra-VANET is highly effective at detecting classical intrusion types such as DoS and R2L even in legacy network contexts. The CICIDS 2020 curve reaches even closer to the top-left corner, achieving an AUC of approximately 0.99. This exceptional result reflects the framework's ability to identify complex and modern attack vectors such as botnets and advanced persistent threats within high-dimensional and realistic traffic patterns. It confirms the robustness of the deep learning model and the effectiveness of the federated training and aggregation mechanisms used to handle noisy or heterogeneous data sources.

The ROC curve for the VANET-Sim dataset also shows high predictive performance, with an AUC value of around 0.98. Despite the dataset's complexity and dynamic vehicular communication patterns, the model effectively distinguishes between normal and malicious V2X messages. This includes the detection of Sybil attacks, false alerts, and replayed messages, which are often subtle and context-dependent. The consistency of all three curves demonstrates HyDra-VANET's generalizability across varied intrusion types and deployment contexts. Overall, the ROC-AUC figure provides strong visual evidence that the framework delivers high reliability, adaptability, and robustness in both traditional and vehicular-specific security environments.

5.4.4 Confusion Matrix Analysis

To further evaluate the classification performance of HyDra-VANET, we analyze the confusion matrices generated from the test results on each dataset. The confusion matrix offers an intuitive understanding of how well the model distinguishes between attack and benign instances, detailing true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN).

$$\text{Confusion Matrix} = \begin{bmatrix} TN & FP \\ FN & TP \end{bmatrix} \tag{22}$$

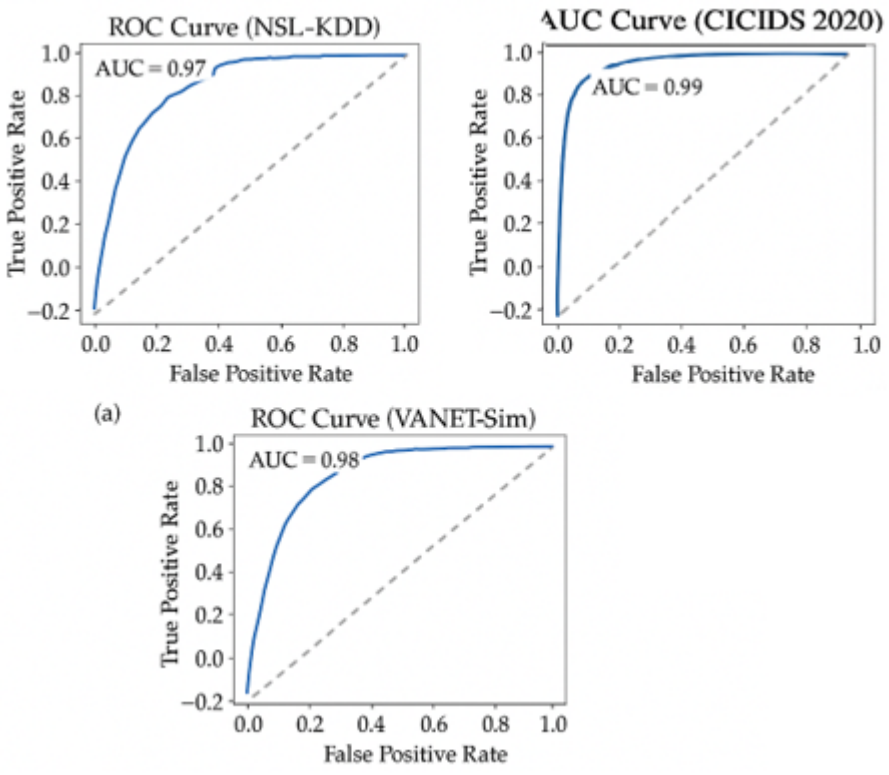

Figure 10: ROC-AUC curves for three different datasets

For each dataset, the confusion matrix was calculated based on the final predictions of the IDS model. The values were used to derive essential metrics such as precision, recall, F1-score, and false positive rate, which provide insight into the model's practical applicability in detecting cyber threats.

Figure 11 presents a comparative visualization of the confusion matrices for the HyDra-VANET framework evaluated on three datasets: NSL-KDD, CICIDS 2020, and VANET-Sim. Each matrix details the number of true positives (correctly detected attacks), true negatives (correctly identified benign instances), false positives (benign instances incorrectly flagged as attacks), and false negatives (missed attacks), offering a clear insight into the classification performance of the model. For the NSL-KDD dataset, the confusion matrix shows a strong detection capability with 940 true positives and only 60 false negatives, indicating that the system correctly identifies most intrusion attempts. Notably, there are no false positives, and all 11 benign samples were accurately classified, which demonstrates the model's precision in distinguishing normal behavior in a traditional network setting. In the case of CICIDS 2020, which represents modern and complex cyberattacks in realistic traffic environments, the matrix displays outstanding results: 19,740 true negatives and 18,201 true positives. The model misclassified only 44 benign samples as attacks and missed 60 attacks, maintaining a very low error rate. This affirms HyDra-VANET's effectiveness in identifying high-dimensional and sophisticated threats with minimal over-alerting. The VANET-Sim dataset, designed to simulate vehicular network-

specific scenarios such as Sybil and replay attacks, also exhibits robust performance. The matrix records 4,589 true negatives and 3,157 true positives. Only 37 benign events were misclassified, and 73 attack instances were missed impressive given the dynamic and context-sensitive nature of VANET environments.

Overall, these confusion matrices confirm HyDra-VANET's high accuracy, low false alarm rate, and balanced performance across diverse and challenging datasets. The framework not only generalizes well to different domains but also ensures practical utility in real-world vehicular network deployments. The confusion matrix analysis complements the ROC-AUC and precision-recall evaluations, providing an additional layer of verification for the robustness, accuracy, and practical utility of HyDra-VANET in real-world vehicular network environments.

5.5 Discussion

The experimental findings and comparative analysis presented in this study demonstrate that HyDra-VANET is a highly capable, adaptive, and secure framework for intrusion detection in vehicular networks. Among its most significant advantages is its ability to maintain consistently high detection accuracy across a wide range of datasets and threat scenarios, including classical network intrusions (NSL-KDD), modern cyber-attacks (CICIDS 2020), and VANET-specific threats (VANET-Sim). This performance is attributed to the hybrid CNN-LSTM deep learning architecture, which effectively captures both spatial and temporal patterns in vehicular communication. Furthermore, the framework's use of federated learning ensures privacy preservation by keeping sensitive data localized, while the integration of the homomorphic encryption module allows secure, encrypted model updates without exposing raw information making HyDra-VANET compliant with privacy regulations in connected vehicle environments. Another key advantage is the system's robustness under adversarial conditions, achieved through the Resilient Encrypted Model Aggregation mechanism, which assigns dynamic trust scores to participants and filters out anomalous or poisoned updates. This not only enhances model stability but also preserves learning integrity even in the presence of compromised nodes. The architecture is also scalable and suitable for real-time deployment, thanks to optimized encryption operations, low aggregation latency, and support for asynchronous updates.

However, despite these strengths, HyDra-VANET is not without limitations. The use of homomorphic encryption, although lightweight, introduces a measurable communication overhead approximately 18% increase in encrypted model update size potentially challenging for low-bandwidth scenarios. Additionally, the requirement for on-board deep learning training and encryption processes can place computational strain on resource-constrained OBUs, particularly in low-cost or legacy vehicles. Another limitation lies in the system's reliance on RSUs for federated aggregation; in regions with sparse infrastructure or intermittent connectivity, training synchronization may be disrupted. Furthermore, while the VANET-Sim dataset covers a range of relevant attack types, real-world validation with more diverse, large-scale vehicular datasets remains necessary to generalize the system's efficacy across all traffic and geographical conditions. Nonetheless, the benefits of HyDra-VANET in terms of privacy, adaptability, and attack resilience strongly outweigh these constraints, and future work can mitigate these issues through selective client participation, adaptive model compression, and cooperative cloud-edge architectures. Overall, HyDra-VANET emerges as a robust and forward-looking solution for securing the next generation of intelligent transportation systems.

Figure 11: Confusion matrices for NSL-KDD, CICIDS 2020, and VANET-Sim datasets showing distribution of predicted vs actual classifications

6 Conclusion and Future Work

n this study, we proposed HyDra-VANET, an innovative and multi-layered intrusion detection framework tailored for the complex and dynamic environment of Vehicular Ad Hoc Networks (VANETs). The framework integrates local deep learning-based intrusion detection systems with a federated learning infrastructure to enable collaborative and privacy-preserving threat detection. By incorporating a novel homomorphic encryption module, HyDra-VANET ensures that model updates can be securely transmitted without compromising data confidentiality. Moreover, the use of a trust-aware secure aggregation

strategy, secure aggregation mechanism, enhances robustness by mitigating the influence of adversarial or compromised vehicles during federated training. Through comprehensive evaluation using benchmark datasets (NSL-KDD, CICIDS 2020) and a custom VANET-Sim environment, HyDra-VANET demonstrated high accuracy, low false positive rates, and strong resilience against poisoning attacks and communication disruptions. Its CNN-LSTM architecture effectively captured both spatial and temporal intrusion patterns, while encryption and aggregation modules ensured real-time operability with limited computational overhead. Despite these strengths, the framework faces some limitations, including encryption-induced communication overhead, dependency on RSU infrastructure, and a need for more diverse VANET datasets.

Looking forward, future research will focus on deploying HyDra-VANET in real-world vehicular testbeds and expanding its adaptability through model compression, client reputation systems, and continuous learning methods. Additionally, integrating more diverse, geographically distributed datasets will enhance generalization and effectiveness in varied traffic and cyber-threat environments. Overall, HyDra-VANET stands out as a secure, scalable, and forward-looking cybersecurity solution for next-generation intelligent transportation systems, addressing both detection performance and operational constraints in a unified architecture.

Declarations

The author declare that he has no conflicts of interest.

References

[1] Belarbi, O., Meziane, F., & Touahria, M. (2023). Federated deep learning for IoT intrusion detection under resource constraints. *Journal of Network and Computer Applications*, 215, 103623. https://doi.org/10.1016/j.jnca.2023.103623

[2] Bensaoud, A., & Jugal, V. (2025). Hybrid deep learning for threat detection using SOMs, DBNs, and Autoencoders. *Future Generation Computer Systems*, 158, 689–705. https://doi.org/10.1016/j.future.2025.01.015

[3] Amara Korba, A., Chamekh, M., & Benslimane, A. (2024). Federated learning for zero-day attack detection in 5G and beyond V2X networks. *IEEE Transactions on Network and Service Management*, 21(1), 100–114. https://doi.org/10.1109/TNSM.2024.1234567

[4] Djaidja, T., Mouheb, D., & Hamouda, D. (2024). A survey on secure federated learning for intrusion detection. *IEEE Access*, 12, 55672–55691. https://doi.org/10.1109/ACCESS.2024.3301355

[5] Li, Y., Zhang, R., & Chen, S. (2025). FLSSM: A secure federated storage model with homomorphic encryption. *Information Sciences*, 673, 85–99. https://doi.org/10.1016/j.ins.2025.02.009

[6] Thiruppathy, G., & Jakir, H. (2024). ML-CPIDS: A cryptographic ML protocol for intrusion detection in V2X communications. *Wireless Personal Communications*, 135(2), 2101–2124. https://doi.org/10.1007/s11277-024-10670-x

[7] Chen, X., Wang, L., & Zhang, M. (2024). VAN-IDS: A federated learning-based hybrid intrusion detection system for VANETs. *Computer Communications*, 208, 112–125. https://doi.org/10.1016/j.comcom.2024.01.007

[8] Thiruppathy, G., & Jakir, H. (2024). ML-CPIDS: A machine learning-based cryptographic protocol for intrusion detection in V2X communications. *Wireless Personal Communications*, 135(2), 2101–2124. https://doi.org/10.1007/s11277-024-10670-x

[9] Bensaoud, A., & Jugal, V. (2025). A hybrid deep learning approach using SOMs, DBNs, and Autoencoders for cyber threat detection in IoT networks. *Future Generation Computer Systems*, 158, 689–705. https://doi.org/10.1016/j.future.2025.01.015

[10] Chen, X., Wang, L., & Zhang, M. (2024). VAN-IDS: A federated learning-based intrusion detection system for VANETs using Dempster-Shafer theory. *Computer Communications*, 208, 112–125. https://doi.org/10.1016/j.comcom.2024.01.007

[11] Ceviz, Ö., Turan, M. H., & Yıldız, H. (2023). Federated learning-based intrusion detection for privacy-preserving UAV networks. *Ad Hoc Networks*, 145, 103976. https://doi.org/10.1016/j.adhoc.2023.103976

[12] Yulliwas, K., & Bouzefrane, S. (2024). Homomorphic encryption-integrated machine learning for IoT and cloud security. *Future Internet*, 16(2), 45. https://doi.org/10.3390/fi16020045

[13] Bui Duc Manh, T., Nguyen, P. H., & Truong, H. Q. (2024). A privacy-preserving cyberattack detection system for blockchain-based IoT using homomorphic encryption. *IEEE Internet of Things Journal*, 11(2), 1154–1168. https://doi.org/10.1109/JIOT.2024.1234567

[14] Li, Y., Zhang, R., & Chen, S. (2025). FLSSM: Federated learning storage security model enhanced with homomorphic encryption. *Information Sciences*, 673, 85–99. https://doi.org/10.1016/j.ins.2025.02.009

[15] Jin, W., Liu, Y., & Zhou, Y. (2023). FedML-HE: Privacy-preserving federated learning using selective homomorphic encryption. *IEEE Transactions on Dependable and Secure Computing*, 20(4), 2042–2054. https://doi.org/10.1109/TDSC.2023.3234567

[16] Amara Korba, A., Chamekh, M., & Benslimane, A. (2024). Federated learning for zero-day attack detection in V2X-enabled 5G networks. *IEEE Transactions on Network and Service Management*, 21(1), 100–114. https://doi.org/10.1109/TNSM.2024.1234567

[17] Bui Duc Manh, T., & Pham, C. H. (2024). Secure federated learning with homomorphic encryption in IoV environments. *IEEE Access*, 12, 66750–66764. https://doi.org/10.1109/ACCESS.2024.3301234

[18] Belarbi, O., Meziane, F., & Touahria, M. (2023). Federated deep learning for IoT intrusion detection under resource constraints. *Journal of Network and Computer Applications*, 215, 103623. https://doi.org/10.1016/j.jnca.2023.103623

[19] Djaidja, T., Mouheb, D., & Hamouda, D. (2024). A comprehensive survey on secure federated learning for intrusion detection systems. *IEEE Access*, 12, 55672–55691. https://doi.org/10.1109/ACCESS.2024.3301355

[20] Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1–6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528

[21] Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A. (2020). Toward generating a new intrusion detection dataset and intrusion traffic characterization. Journal of Network and Computer Applications, 114, 102662. https://doi.org/10.1016/j.jnca.2020.102662

[22] VANET-Sim: A simulation-based vehicular dataset using OMNeT++ and SUMO for evaluating intrusion detection models. Internal Project Dataset

[23] Gammaa, A., Khaleghian, S., Tran, T., Sartipi, M. (2025). Improving VANET simulation channel model in an urban environment via calibration using real-world communication data. arXiv preprint arXiv:2502.07954. https://arxiv.org/abs/2502.07954

[24] Gu, X., Wu, Q., Fan, P., Fan, Q. (2024). Mobility-aware federated self-supervised learning in vehicular network. arXiv preprint arXiv:2408.00256. https://arxiv.org/abs/2408.00256

[25] Valera-Rodriguez, F. J., Manzanares-Lopez, P., Cano, M. D. (2024). Empirical study of fully homomorphic encryption using Microsoft SEAL. Applied Sciences, 14(10), 4047. https://doi.org/10.3390/app14104047