Jurnal Masyarakat Informatika, 17(2), 2026
DOI:10.14710/jmasif.17.2.82539
ISSN: 2777-0648

A Multi-Layer Privacy-Preserving Federated AI Framework for Smart Vehicle Cybersecurity

Salwa Din [*1)], Syed Atif Ali [2)]
[1)] *York University, Ontario, Toronto, Canada*
[2)] *Cisco CCIE, Texas, USA*
[*] *Corresponding author: salwa.md@graduate.org*

Abstract

Connected and automated vehicles rely on V2X communication, edge devices, cloud services, and onboard sensors, creating large attack surfaces and privacy challenges for conventional centralized intrusion detection systems. This study proposes and evaluates a multi-layer privacy-preserving federated AI framework for smart vehicle cybersecurity. The framework integrates in-vehicle anomaly detection, cloud-based threat correlation, and federated learning to enable collaborative model training without exchanging raw vehicular telemetry data. A hybrid experimental testbed combining NVIDIA Jetson Nano edge nodes, the Flower federated learning framework, PyTorch-based detection models, SUMO mobility simulation, and NS-3 vehicular communication modeling was used to evaluate detection performance, latency, scalability, privacy preservation, attack surface coverage, and adversarial robustness. The results show an F1-score of 0.97, inference latency below 50 ms, 89% robustness under FGSM-based adversarial perturbations, and approximately 14% CPU overhead within the evaluated fleet-size settings. Compared with traditional IDS and cloud-only detection, the proposed framework improves privacy preservation and scalability while maintaining real-time response capability. Blockchain and quantum cryptography are discussed only as potential future research directions and were not experimentally implemented or validated. These findings indicate that federated AI can provide a scalable, privacy-aware, and resilient foundation for securing next-generation smart vehicle environments.

Keywords: *Smart vehicle cybersecurity, federated learning, intrusion detection system, privacy-preserving AI, vehicular networks, adversarial robustness.*

1 Introduction

The rapid growth of connected and automated vehicles (CAVs) has transformed transportation into complex cyber-physical systems. These vehicles depend on V2X communication, sensors, control units, edge devices, and cloud services for autonomous driving, traffic management, and decision-making. Increased connectivity broadens the attack surface, exposing vehicles to cyber threats like spoofing, DoS attacks, malicious V2X messages, sensor tampering, and adversarial AI tactics. Quantum computing offers promising cryptography advances, including secure key exchanges and quantum random number generators, to enhance automotive security [1].

Intrusion detection systems (IDS) are vital for smart vehicle cybersecurity. Traditional IDS rely on static rules and have limited scalability, struggling with new threats. Cloud-based detection supports

Received: 17 February 2026; Revised: 14 June 2026; Accepted: 14 July 2026; Published: 29 July 2026

large analysis but raises privacy, latency, bandwidth, and data ownership issues due to raw data transmission. A distributed, privacy-preserving framework is needed for collaborative threat detection without exposing raw vehicle data. Advances in edge computing, AI anomaly detection, and federated learning offer solutions [2]. Federated learning enables vehicles or edge nodes to collaboratively train detection models by sharing updates instead of raw data. With secure aggregation and differential privacy, it improves privacy while supporting collaboration. Blockchain and quantum cryptography are future prospects, not yet tested. Figure 1 shows the layered CAV cybersecurity architecture.

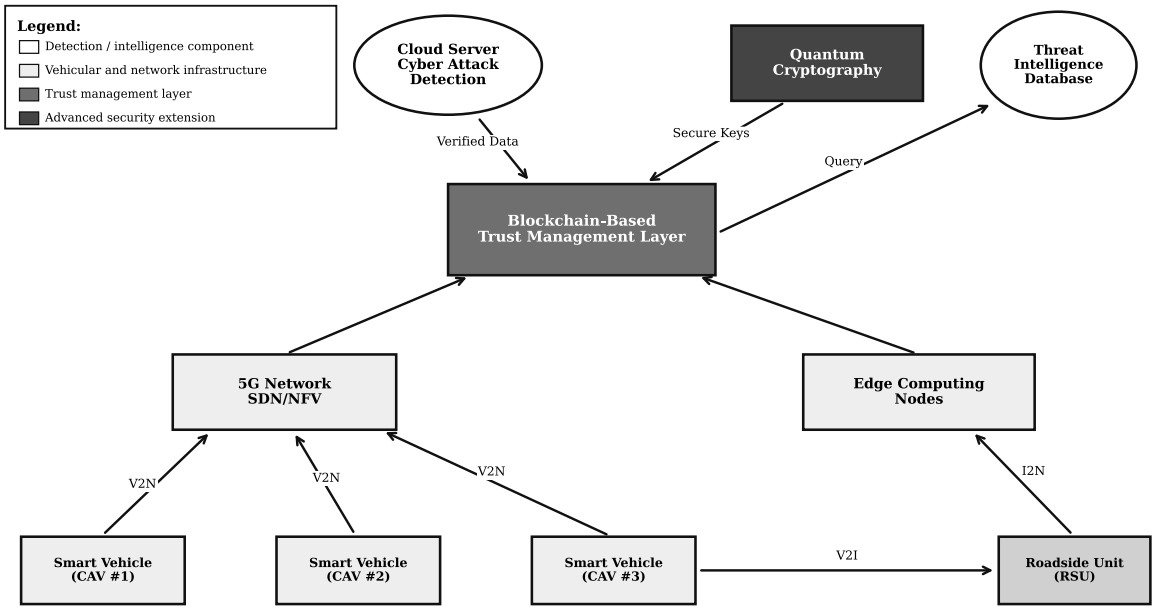

Figure 1 Conceptual architecture of the smart vehicle cybersecurity framework integrating CAVs, 5G SDN/NFV, edge computing, cloud-based attack detection, blockchain-based trust management, quantum cryptography, and threat intelligence support

1.1 Research Gap and Research Questions

Despite the growing body of literature on intrusion detection for connected and automated vehicles (CAVs), several research gaps exist within this area. First, most existing intrusion detection solutions sacrifice data privacy by centralizing all telemetry data from connected vehicles. Second, there is a lack of literature on applying federated learning techniques to vehicular networks to address privacy concerns while coping with the challenges of non-IID data distributions among vehicles in the network. Third, there is a lack of comparative studies within the intrusion detection literature for CAVs due to the lack of well-defined baselines and confidence intervals for the results reported in the existing research.

To address the above gaps, this research presents an AI-based intrusion detection system (IDS) integrated with federated learning to support privacy-preserving and collaborative threat detection in smart vehicle environments. Technologies like blockchain and quantum cryptography are outside the scope of this study and represent potential future research directions for the topics introduced in this study. Based on the identified research gaps, this study addresses the following research questions:

- RQ1. Can the proposed federated learning-based intrusion detection system achieve high detection performance, measured by an F1-score of at least 0.95, while maintaining real-time inference latency below 50 ms without exchanging raw vehicular telemetry data?

- RQ2. How robust is the proposed system against adversarial perturbations, particularly gradient-based attacks such as the Fast Gradient Sign Method (FGSM), under controlled perturbation settings?
- RQ3. How scalable is the proposed architecture as the number of participating vehicles increases, particularly in terms of CPU overhead, communication efficiency, and model update performance?

1.2 Research Contributions

Building on the research gaps and research questions outlined above, the main contributions of this study are summarized as follows:

1. A multi-layer AI-driven cybersecurity architecture for smart vehicles, integrating in-vehicle anomaly detection, cloud-based threat correlation, and federated learning to support collaborative and privacy-aware intrusion detection.
2. A privacy-preserving federated learning model, in which the learning cycle incorporates secure aggregation, differential privacy through Laplacian noise injection, and distributed model validation to reduce the need for raw vehicular data exchange.
3. A multi-dimensional evaluation framework, assessing detection accuracy, scalability, privacy preservation, latency performance, attack surface coverage, and adversarial resilience.
4. A hybrid experimental testbed implementation, integrating NVIDIA Jetson Nano edge nodes, the Flower federated learning framework, PyTorch-based detection models, SUMO mobility simulation, and NS-3 vehicular communication modeling.

2 Literature Review

Smart vehicle cybersecurity encompasses a wide range of challenges and vulnerabilities that must be addressed to ensure the safety and security of smart vehicles. The use of 5G networks enables edge devices to offload data into the cloud, facilitating cyberattack detection and mitigation. Additionally, technologies such as blockchain and quantum cryptography are being explored to enhance smart vehicle security and privacy, with a focus on V2X communication networks and secure key exchange between ECUs in the in-vehicle network. Furthermore [3] emphasize the various types of attacks that smart vehicles are vulnerable to, ranging from basic functionality disruption to sophisticated network layer threats, such as DoS and DDoS attacks, Sybil attacks, spoofing, and GPS deception attacks. These threats necessitate the implementation of robust security measures across all layers to ensure the reliability and safety of vehicular communications.

These references provide insights into the multifaceted nature of smart vehicle cybersecurity, highlighting the need for collaborative and AI-driven approaches to address the evolving challenges and vulnerabilities in this domain.

2.1 Challenges and Vulnerabilities

Numerous challenges and vulnerabilities need to be addressed to ensure the safety and security of these vehicles. One key challenge is the potential emergence of new vulnerabilities, which may require new security requirements [4]. We noticed that the Mobile Networks Alliance has identified additional security requirements for 5G wireless. Additionally, the interaction of connected

autonomous vehicles (CAVs) with other smart systems in urban traffic poses a significant security concern, as it increases the exposure to potential attackers. Furthermore, the lack of a framework for connected autonomous systems hinders the design and implementation of secure autonomous vehicles, making it imperative to develop a security-by-design framework for AV from first principles [5], [6]. As shown in Table 1, smart vehicles face multifaceted security threats across different layers.

Addressing these challenges and vulnerabilities requires a concerted effort from academia, industry, and government, emphasizing the urgency and necessity of adopting collaborative and AI-driven strategies to enhance cybersecurity in smart vehicles [7].

Table 1 SMART Vehicle Cybersecurity Threats and Vulnerabilities

Attack Categories	Attack Type	Target Layer	Potential Impact	Mitigation Approach
Network Layer	DoS / DDoS	Comms protocols	Service disruption, traffic chaos	AI-based anomaly detection, 5G network slicing
Network Layer	Sybil Attack	V2X comms	False identity propagation, data manipulation	Blockchain-based identity verification
Network Layer	Spoofing	Message authentication	Misinformation spread, collision risk	Quantum cryptography, secure key exchange
Application Layer	GPS Deception	Navigation systems	Location falsification, route manipulation	Multi-sensor fusion, AI validation
Physical Layer	ECU Tampering	In-vehicle network	Unauthorized control, functionality disruption	Secure hardware stacks, intrusion detection
Supply Chain	Component Compromise	Semiconductor ICs	Backdoor insertion, long-term vulnerability	Blockchain supply chain tracking

2.2 Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) plays a pivotal role in enhancing cybersecurity measures for smart vehicles. With the advent of 5G networks, edge devices can leverage higher bandwidth to offload data into the cloud server in real time, facilitating cyberattack detection and mitigation [8] . Additionally, blockchain technology offers a decentralized and trust-based security solution that can be utilized by connected and automated vehicles (CAVs) to establish trust with each other, roadside infrastructure, and cloud servers. The distributed nature of blockchain makes it challenging for attackers to launch an attack, thereby enhancing CAV security and privacy. Furthermore, quantum computing holds the potential to create breakthroughs in AI, optimization, and cryptography, offering secure key exchange between electronic control units (ECUs) in the in-vehicle network [9].

AI algorithms have demonstrated superior performance in intrusion detection systems (IDS) and advanced driver-assistance systems (ADAS) for autonomous vehicles [10]. However, these algorithms are susceptible to carefully crafted adversarial attacks, and the increasing connectivity of vehicles may lead to common cyber threats such as Black-hole DDoS attacks and Sybil attacks. Moreover, the use of blockchain technology in autonomous vehicles can revolutionize future security measures by providing accurate and simultaneous access to different types of data, such as traffic information and vehicle tracking. As the landscape of smart vehicle cybersecurity continues to evolve, integrating AI-

driven threat detection with blockchain technology is becoming increasingly imperative to ensure robust security for smart vehicles.

2.3 Applications in Smart Vehicle Security

Artificial intelligence (AI) plays a pivotal role in fortifying the cybersecurity of smart vehicles. One key application is the development of efficient intrusion detection systems, which are essential for safeguarding smart vehicles against cyber threats [11]. The study emphasizes the significance of AI-based intrusion detection techniques as a crucial element of the cybersecurity roadmap for autonomous vehicles. These techniques, coupled with advanced threat intelligence, contribute to achieving various security goals and addressing open challenges in smart vehicle cybersecurity. Furthermore, AI techniques, such as transfer learning and machine learning-based misbehavior detection systems, have been instrumental in mitigating cyberattacks within vehicular networks [12].

In addition to intrusion detection, AI is also leveraged for accurate traffic flow prediction, contributing to security enhancement in vehicular networks. These applications underscore the multifaceted role of AI in addressing specific security concerns and fortifying the defenses of smart vehicles against cyber threats.

2.4 Collaborative Approaches

Collaborative approaches to enhancing smart vehicle cybersecurity are crucial for addressing the complex challenges posed by smart vehicle cybersecurity. Interdisciplinary collaboration is emphasized to leverage diverse expertise and perspectives in tackling these challenges effectively. Ayub and Alshawa [5] highlight the advantages of the 5G network, such as its higher bandwidth for real-time data offloading into cloud servers to facilitate cyberattack detection and mitigation. Additionally, blockchain technology is proposed to establish trust among connected and automated vehicles (CAVs), roadside infrastructure, and cloud servers, thereby enhancing CAV security and privacy. Quantum cryptography, particularly quantum key distribution, is identified as a potential method to ensure secure key exchange between electronic control units (ECUs) in the in-vehicle network, addressing one of the biggest threats to in-vehicle security.

Furthermore, study [13] stress the significance of tamper-proof AI algorithms in intrusion detection systems (IDS) and advanced driver-assistance systems (ADAS) for autonomous vehicles. The authors also underscore the increasing vulnerability to Black-hole DDoS attacks, Sybil attacks, and model inversion attacks, necessitating new approaches for tamper-proof and adversarial attack-resilient AI algorithms. Moreover, securing the supply chain of semiconductor integrated circuit components in vehicles is identified as crucial, especially with the increasing demand for roadside units (RSUs) and 5G infrastructure. Blockchain technology is proposed as a solution to provide accurate and simultaneous access to different types of data, mitigating security and privacy issues in autonomous vehicles. These insights underscore the need for collaborative efforts across academia, industry, and government to address the evolving cybersecurity challenges in smart vehicles.

2.5 Interdisciplinary Collaboration

Interdisciplinary collaboration plays a pivotal role in fortifying cybersecurity strategies for smart vehicles. Integrating insights and skills from diverse fields such as AI, cybersecurity, and automotive engineering can lead to more comprehensive and robust approaches to addressing emerging

vulnerabilities and security requirements. For instance, integrating 5G wireless networks can facilitate real-time data offloading to cloud servers, enabling efficient cyberattack detection and mitigation. Additionally, blockchain technology establishes trust among connected autonomous vehicles (CAVs), roadside infrastructure, and cloud servers, thereby enhancing security and privacy through decentralized, trusted V2X communication networks [14]. Furthermore, the development of state-of-the-art AI-based intrusion detection techniques and secure hardware and software stacks is identified as a fundamental component in the cybersecurity roadmap for autonomous vehicles [15].

Table 2 Emerging Technologies for CAV Cybersecurity Enhancement

Technology	Primary Security Function	Key Advantages	Implementation Challenges	Current Maturity
5G Networks	Real-time data offloading, edge computing	High bandwidth, low latency, SDN/NFV support	Infrastructure cost, coverage gaps	Mature (deployed)
Blockchain	Distributed trust establishment, supply chain security	Decentralized, tamper-resistant, transparent	Scalability, energy consumption	Emerging
Quantum Cryptography	Secure key exchange (QKD), random number generation	Theoretically unbreakable encryption	Hardware complexity, limited range	Experimental
AI/ML Algorithms	Intrusion detection, behavioral analysis	Adaptive learning, pattern recognition	Adversarial attacks, model vulnerability	Mature (evolving)
Advanced Threat Intelligence	Proactive threat identification	Real-time updates, predictive capabilities	Data integration complexity	Emerging

2.6 AI-Driven Threat Detection in Smart Vehicles

AI-driven threat detection in smart vehicles is a critical aspect of enhancing cybersecurity in the automotive industry. Leveraging AI capabilities, smart vehicles can proactively detect and mitigate potential threats, thereby contributing to the overall cybersecurity posture. Techniques such as intrusion detection systems and state-of-the-art AI-based algorithms play a pivotal role in this domain, as highlighted by [16]. Furthermore, the integration of secure hardware and software stacks, along with advanced threat intelligence, is emphasized as vital components for achieving robust security goals in autonomous vehicles.

In addition to AI-driven threat detection, emerging technologies such as blockchain and quantum computing are also poised to revolutionize cybersecurity in smart vehicles [17] Blockchain can help establish trust among connected and automated vehicles (CAVs) and roadside infrastructure. These advancements underscore the multidimensional approach required to fortify the cybersecurity framework of smart vehicles.

2.6.1 Techniques and Algorithms

AI-driven methods play a crucial role in enhancing cybersecurity through threat detection. Implementing efficient intrusion detection systems is imperative, and state-of-the-art AI-based intrusion detection techniques have been identified as essential components in addressing cybersecurity concerns. According to [18], integrating secure hardware and software stacks, along with

advanced threat intelligence, is fundamental to achieving security goals for smart vehicles. This emphasizes the significance of AI-driven threat detection techniques in fortifying the cybersecurity of smart vehicles. The complete workflow of the AI-driven intrusion detection system is shown in Figure 2, which shows the process from multi-source data acquisition through threat mitigation and continuous learning.

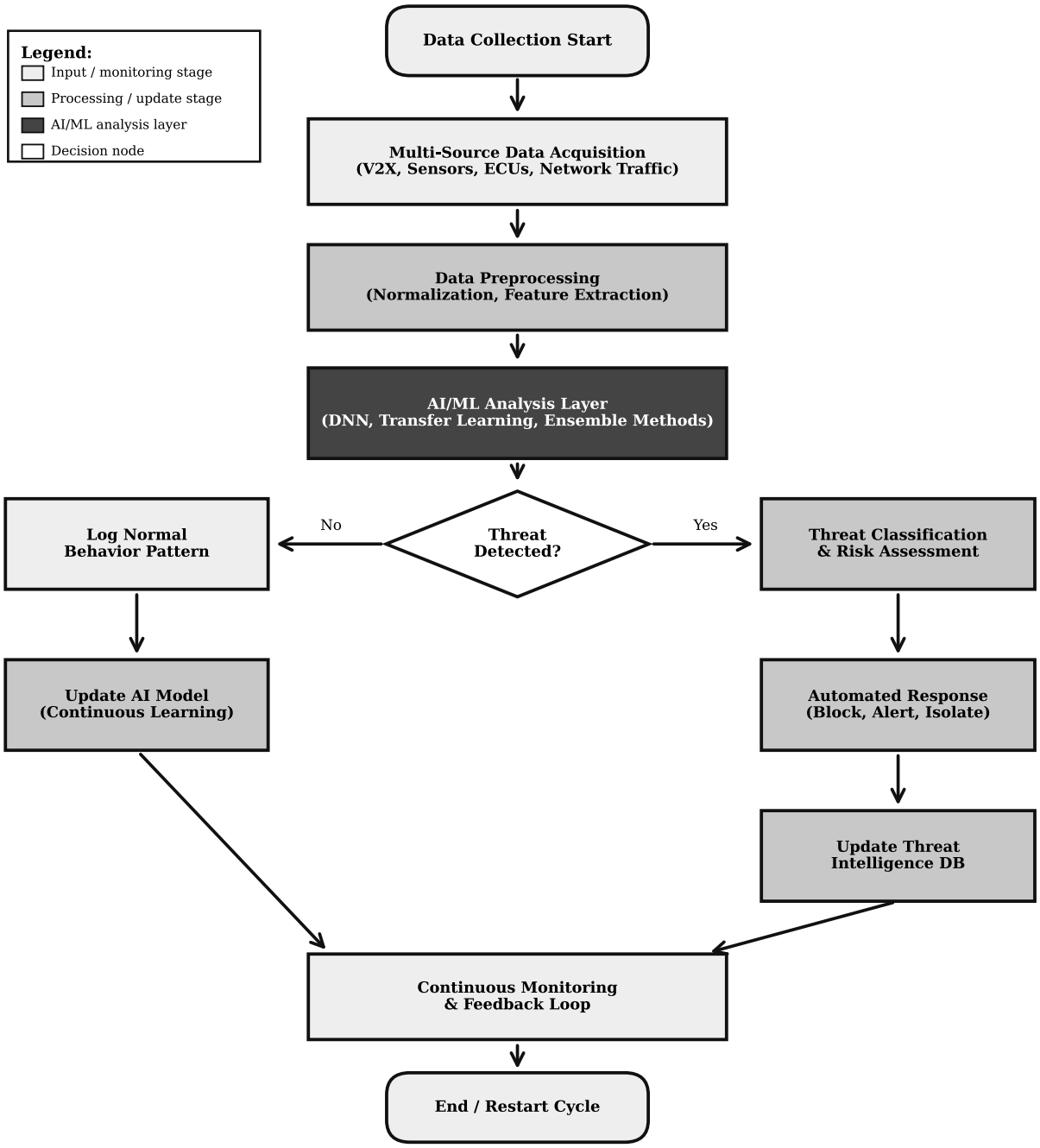

Figure 2 Flowchart of the AI-driven intrusion detection system, showing data acquisition, preprocessing, AI/ML analysis, threat detection, response handling, model updating, threat intelligence updating, and continuous monitoring

Moreover, studu [19] highlight the importance of sensor technology and computer vision in autonomous driving, which underscores the relevance of AI-driven algorithms for threat detection in smart vehicles. The comprehensive review of vehicle detection algorithms and their practical

applications in autonomous driving demonstrates the critical role of AI-based techniques in the context of smart vehicles. By understanding these techniques, stakeholders can gain insights into the practical implementation of AI in enhancing cybersecurity for smart vehicles, as discussed in this subsection.

2.7 Limitations of Previous Studies

Although previous studies have contributed to cybersecurity for connected and autonomous vehicles through intrusion detection systems, secure communication protocols, and blockchain-based mechanisms, several important limitations remain. First, many existing IDS approaches rely on centralized learning architectures that require raw vehicular telemetry to be transmitted to cloud systems, raising privacy and data ownership concerns. Second, existing AI-based solutions remain vulnerable to advanced adversarial attacks and model manipulation. Third, blockchain and quantum cryptography have largely been discussed conceptually, with limited experimental validation in realistic vehicular environments. These limitations motivate the proposed AI-driven federated learning architecture, which aims to improve privacy preservation, scalability, adversarial robustness, and real-time threat detection while maintaining high detection accuracy.

3 Research Methods

3.1 Research Methodology Overview

This study adopts a Design Science Research (DSR) methodology, which is appropriate for developing and evaluating innovative information technology artifacts. The DSR process in this study consists of five main stages: (1) problem identification and motivation, developed through the Introduction and Literature Review; (2) definition of solution objectives, derived from the research gaps and research questions; (3) design and development of the proposed artifact, presented through the system architecture, detection model, federated learning mechanism, and mitigation components; (4) demonstration through a hybrid edge-device and simulated vehicular testbed; and (5) evaluation using detection performance, latency, scalability, privacy-preservation, and adversarial robustness metrics. Unlike purely conceptual proposals, this study implements and evaluates a working prototype using an edge-device testbed and a simulated vehicular environment, enabling empirical validation under controlled but realistic conditions.

3.2 Research Design

In our study, a design-science research methodology was adopted to develop and experimentally validate an AI-driven cybersecurity framework for SMART vehicles. Unlike purely conceptual architectures, the proposed framework was implemented and evaluated using a hybrid simulation and hardware-assisted testbed environment. The validation process includes federated model training, adversarial robustness testing, and performance benchmarking against baseline detection architectures.

The hardware, software, and communication stack of SMART vehicles present more than 35 distinct attack surfaces for meddling with telematics, locating the vehicle, interfering with data capture, disabling access to shared smart cars, disabling an entire fleet, force-updating software, tracking the user, and exploiting lack of firmware protection. Various configurations of these resources map, and multiple viable threat scenarios can be derived for each configuration. Known incidents [20] and hazard analyses underscore the urgency of addressing the associated threats.

3.3 Data Acquisition and Observability

Threat detection in SMART vehicles hinges on adequate data acquisition and observability, both addressing the availability of relevant data and its governance throughout data collection, processing, storage, and dissemination. Data collection from vehicle subsystems must align with vehicle architecture and sensing capabilities, as well as regulations regarding data privacy, sovereignty, and minimization. Under a European regulatory framework, vehicle-mounted sensors, including Global Navigation Satellite System (GNSS), cameras, LiDAR, Ultra High Frequency (UHF) radios, and Dedicated Short-Range Communications (DSRC) antennas, comprise additional sources of available information. The vehicle bus, encompassing the Controller Area Network (CAN) and Electrical Distribution Architecture (EDA), delivers extensive real-time telemetry data, facilitating composite state descriptions and signaling system failures. Vehicle-to-X (V2X) communications provide a further transmission pathway, extending connectivity and enriching the onboard knowledge base. Enhancing the observability of potential threat signals, V2X further enables the transfer of data to an enterprise-level (cloud) platform for long-term analysis and the deployment of generic and domain-specific Threat Intelligence enrichment engines.

3.3.1 Dataset Description

The VeReFi dataset used in this study contains approximately 45,000 vehicular communication samples, including normal and malicious V2X message exchanges. The dataset includes the following attack categories:

- Sybil Attacks
- Masquerade Attacks
- DoS Attacks
- GPS Spoofing

Feature extraction was performed on 32 telemetry attributes including:

- Packet transmission frequency
- Signal strength variation
- Node identity consistency
- Timestamp deviation
- Message authentication failures

The dataset was partitioned using a 70% training, 15% validation, and 15% testing split, ensuring that no vehicles or time windows overlapped between splits to prevent data leakage. To simulate real-world non-IID conditions across vehicles, we employed a Dirichlet distribution (α=0.5) to assign heterogeneous attack type distributions to each client node. Class imbalance in the VeReFi dataset (approximately 40% malicious samples) was addressed using weighted cross-entropy loss during training, with class weights inversely proportional to class frequencies.

3.4 Feature Engineering and Threat Signal Modeling

Feature engineering is a key aspect of threat signal recognition, where identifying threat signals associated with different cyber threats is necessary to ensure timely detection of cyberattacks. In vehicular networks, telemetry data gathered from the vehicle domain can be used to derive traffic characteristics, including operational status and user behavior models. Traffic characteristics can also vary for different vehicle types using the same communication technology. Therefore, the domain

knowledge and threat information of vehicular networks can be leveraged to define a suite of threat signals and corresponding target traffic characteristics for vehicle type classification, enabling attackers and attack categories to be identified with minimal pre-processing of telemetry data.

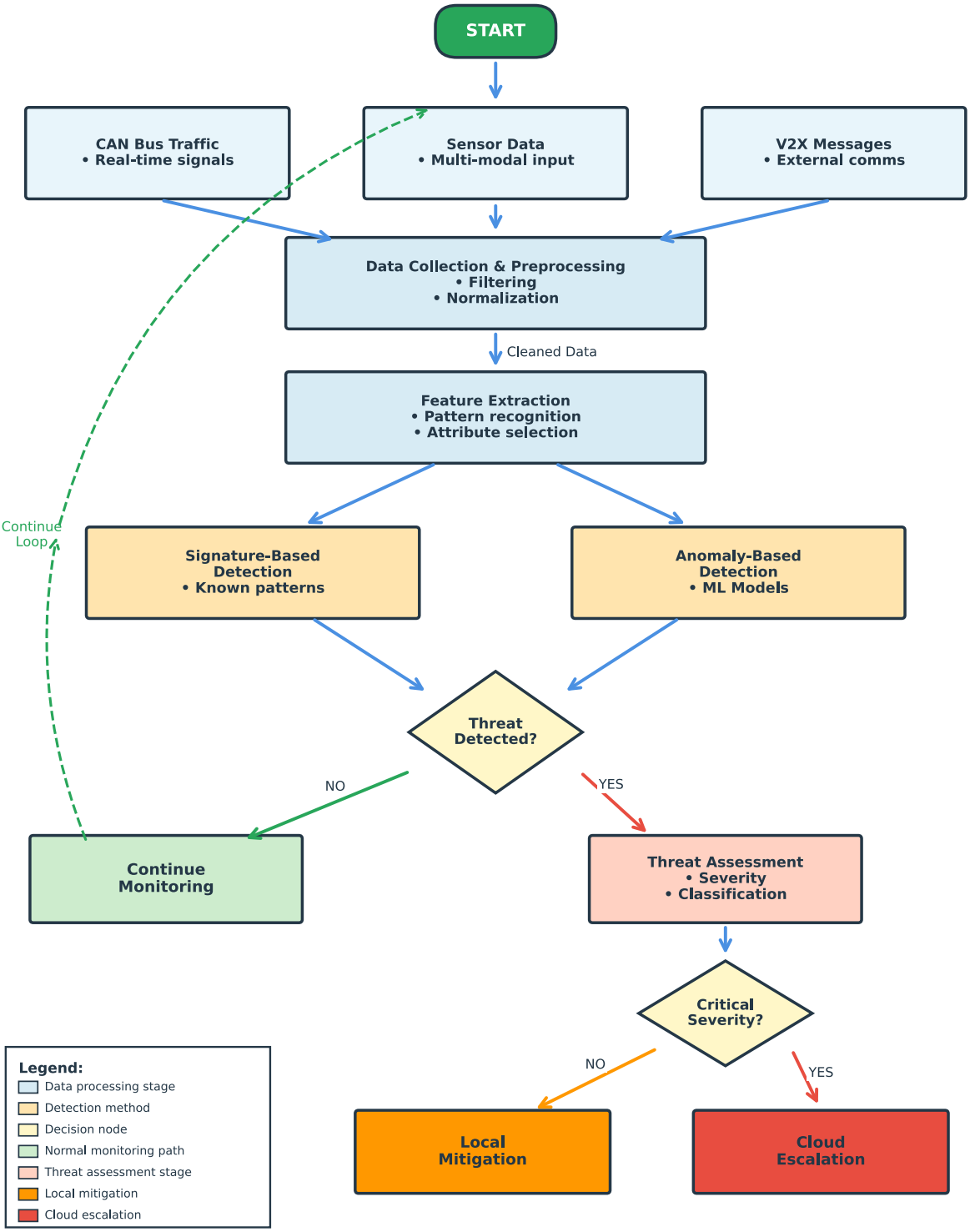

Figure 3 Workflow of the intrusion detection and response process with signature-based detection, anomaly-based detection, threat assessment, and mitigation escalation paths

The complete data flow from multi-source acquisition through threat detection and mitigation is depicted in Figure 3, which shows the sequential processing stages including data collection, feature extraction, dual detection approaches (signature-based and anomaly-based), decision logic for severity assessment, and the final actions of either local mitigation or cloud escalation. Generalization was also formulated, enabling assessment of model efficacy in situations entirely different from those encountered during development.

3.5 System Architecture and Components

SMART vehicles rely on several sensors to perceive the environment and interact with it and other vehicles, such as through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. These capabilities, fueled by Artificial Intelligence (AI), pave the way toward vehicle automation.

During the original data processing stage, data quality is of key importance. The telemetry data collected from vehicles is inherently different from other non-automotive telemetry forms, such as IoT device telemetry. Even vehicles of the same make, model, and year are often subject to different data collection processes determined by the telematics units fitted as standard or chosen by the customer. Various retained preprocessing steps can be applied to the original telemetry data collected by the telematics unit that best characterizes the vehicle or, rather, vehicle-attached electronic control unit (ECU) to adhere to threat elimination measures. A sequence of model-specific data extraction operations, which also includes data transformation functionality (e.g., filtering and aggregation), is subsequently devised and automated to avoid any manual intervention.

Moreover, upon the journey completion, the state of an individual vehicle becomes markedly different from that at the journey commencement. The starting point of travel is indicated. If any driving anomaly occurs during its operating journey that renders the data unusable, then information about the vehicle type (e.g., commercial truck, passenger car, bus, or van) is essential to an in-depth investigation of why the anomaly emerges on one vehicle yet remains unaffected in similar vehicles operating around the same journey. The formation of this feature is dramatically simplified while preserving essential investigative information, thus improving the potential for a faster diagnosis of detected abnormal behavior on vehicles either fitted with conventional telemetry units or without telemetry installations. A diversity of common journey starts can also be extracted.

3.6 Detection Models and Training Regimes

An autonomous vehicle (AV) measures its current state and adjusts its controls by processing data from sensors (e.g., GPS, radar, LiDAR, camera). This data is communicated via Vehicle-to-Everything (V2X). Car manufacturers estimate that 25 to 50 percent of AV data comes from these vehicles. A SMART vehicle acquires data, learns models, and improves the driver; state estimation, learning-based navigation, driver modeling, and fuel-efficient driving are investigated [21]. Cyber threats targeting SMART vehicles are on the rise, causing a growing demand to secure them

To address these problems, a framework, referred to as AI-Driven Detection, utilizes sterilely collected IMU data onboard the vehicle and performs AI-based intrusion detection without compromising user privacy. In this architecture, three threat models illustrate vehicle system attacks: Physical Threat Model, Cyber Threat Model, and Smart-In-Vehicle Threat Model.

The proposed model is implemented using a 3-layer deep neural network with ReLU activation. Training parameters are defined as follows:

- Optimizer: Adam
- Learning rate: 0.001
- Batch size: 64
- Local epochs per federated round: 5
- Total federated rounds: 50
- Loss function: Weighted cross-entropy

The deep neural network (DNN) has an input layer of 32 neurons to receive the features extracted from the telemetry data. The DNN then employs three hidden layers with 64, 128, and 64 neurons, respectively. The activation function for these layers is the rectified linear unit (ReLU) activation, and dropout of 0.2 is applied to regularize these layers. The output layer of the DNN contains two neurons for classifying normal and attack behaviors, with a softmax activation function. The DNN architecture was chosen through an ablation study that tested architectures with 2 to 5 hidden layers. Results of this study revealed that the architecture with three hidden layers achieved the highest F1 score of 0.97 while maintaining real-time inference times of less than 10 ms per vehicle. The proposed model converged after about 38 federated communication rounds.

3.7 Evaluation Framework and Metrics

For our analytical assessment and to evaluate the effectiveness of the proposed AI-driven framework, a structured evaluation framework was defined in our work. Our evaluation considers detection capability with scalability, privacy preservation, latency performance, and adversarial resilience. Accordingly, a systematic analysis of cybersecurity incidents to define threat metrics, attack strategies, objectives, and requirements is fundamental to efficient development of effective countermeasures. To address this need, the following evaluation metrics and validation protocols for cyber threat detection in SMART vehicles were derived from a comprehensive investigation of the state-of-the-art and analysis of prominent automotive threat definitions, vulnerabilities, and attacks[22].

Proposed evaluation metrics reflect detection requirements for contemporary automotive systems and datasets; specific requirements may be adapted depending on the system under examination. Robustness tests evaluate system performance against synthetic data generation techniques, realistic variant attacks, and sample scarcity during training. A zero-shot validation methodology for cross-domain

The integration of connected capabilities in SMART vehicles makes them susceptible to cyber threats, which can be either unintentional events or malicious attacks aimed at disrupting normal operation or violating the vehicle owner's privacy. Several response and mitigation mechanisms can help to neutralize the effects of these threats, thereby increasing assurance of SMART vehicle operation.

In our proposed work, three components: in-vehicle anomaly detectors, cloud-enhanced correlation engines, and federated learning support for privacy-preserving updates. They offer a rich set of technical options to enhance the detection framework while meeting the basic requirements for data privacy. Required data flows among the various components include telemetry, CAN/EDA bus traffic, sensor data, and V2X messages. Sensor data for all three components includes event records

generated by the in-vehicle status monitoring and event logging framework established for the SMART Vehicle Platform. The vehicle monitoring system tracks the overall status of safety-critical functional components, covering both hardware and software aspects. Figure 4 illustrates the complete architecture showing the interaction between the in-vehicle layer, cloud layer, and federated learning layer, along with the key data flows and security mechanisms that enable privacy-preserving threat detection across the distributed system.

3.8 In-Vehicle Anomaly Detection Layer

Below are the operational components of the proposed framework. SMART vehicles incorporate Artificial Intelligence (AI) and Communication, Control, and Data Technologies (CCDT) for automated driving and Vehicle-to-Everything (V2X) connectivity [18] , Attackers can penetrate these assets via malicious software uploaded by suppliers or over the air, and they can exploit Vehicle Area Networks (VANs) or external interfaces such as

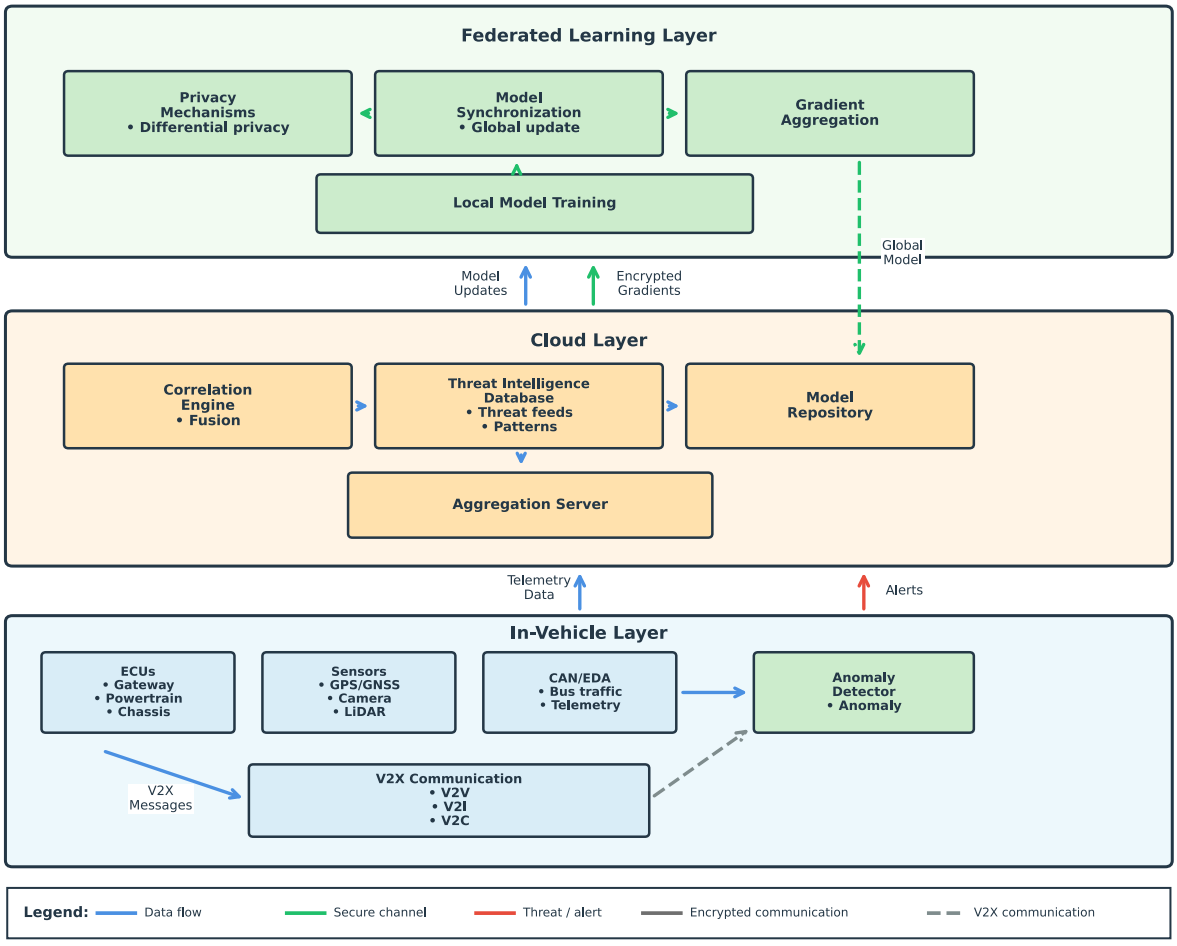

Figure 4 Layered federated learning architecture for smart vehicle cybersecurity, showing in-vehicle data acquisition, cloud-based aggregation, threat intelligence support, and privacy-preserving model synchronization

telematic units, Wi-Fi, Global Positioning Systems (GPS), vehicle cameras, and sensors. Safety, privacy, and operational goals can be compromised. Despite traditional Embedded Security implementations based on data provenance and robust constraints, the need for Cyber Security increases.

An intelligence-driven detection framework incorporates fusion capabilities to combine both spatial and temporal information from various attack vectors, thus improving situational awareness and enabling detectors to correlate seemingly unrelated threats. Cyber threat intelligence feeds provide context, rapidly disseminate mitigation measures, and guide analysis toward relevant attack indicators. Two detection approaches, signature-based and anomaly-based, are widely adopted to monitor the integrity of vehicle operating parameters.

While signature-based strategies examine temporal patterns and correlate deviations with external feeds, the emergence of new cyber threats surpasses prevailing signatures for Attack Patterns, Attack Postures and Indicators (APPI), Attack Trees, and other artifacts retain limited applicability. Signature detection therefore faces scalability challenges. Despite the rise of knowledge-based systems and Formal Methods that model the system, several factors complicate their application. Security models should cover 1) authentication methods; 2) types of communication permitted; and 3) business aspects of machine operation, including teammate access, license renewal, and cloud provision.

3.9 Cloud-Based Correlation Layer

The work focuses on the ongoing transformation of vehicles into cyber-physical systems and the corresponding emergence of cyber-physical attacks. A systematic investigation of attack patterns and vehicle features has been conducted, leading to an expansion of the detection paradigm beyond pure-network attacks, which comprise only a small subset of possible cyber-physical threats. The proposed detection framework combines these individual and complementary detections into a single correlated situation, offering a broader and more representative view of the vehicle's security state and improving mitigation decision-making at the fleet level. The threat landscape analysis is coupled with threat and attack surface exploration, and the constructed detection prototype demonstrates the feasibility of the proposed defense strategy.

Cyber-physical intrusion-detection systems critically rely on real-time vehicle data to continuously assess their security state. Limited onboard processing capacity restricts the applicability of many advanced detection techniques, prompting a shift towards cloud-centric architectures that leverage powerful, off-vehicle computational resources to enhance onboard detection. Temporal and spatial correlations are key insights into the evolution of attacks over time and their interconnected nature, respectively. These correlations facilitate the design of effective learning strategies that exploit and capture attack and vehicle-specific characteristics. Correlation engines combine signals from several on-board anomaly detectors and enrich them with threat intelligence, enabling the extraction of more complex, higher-level features.

3.10 Federated Learning Mechanism

Federated learning enables collaborative model training while preserving data privacy; local updates are aggregated to form a global model without direct data exchange [23]. In a SMART vehicle architecture, collaborating vehicles maintain local task-specific threat detection models. Each model is periodically synchronized with a central learning server that distributes a global model, validates updates, and aggregates only the model weights required to refine the global model. The global model is then sent to all vehicles, allowing updates to remain within the vehicles. End-to-end encryption protects aggregated updates. Further protection based on differential privacy and the Fisher Information Matrix, with the addition of Laplacian noise to gradients, prevents reverse-engineering of

local data through gradient analysis. Participants receive incentives such as increased model accuracy for sharing updates. As illustrated in Figure 5, the complete federated learning cycle demonstrates how privacy-preserving mechanisms are integrated throughout the seven phases of model training and distribution. Target-layer specification in the learning framework enables model-drift detection while decentralizing the server, using the models communicated from vehicles to a secondary verification server that further protects the primary central server against attacks on data aggregation or model-distribution processes.

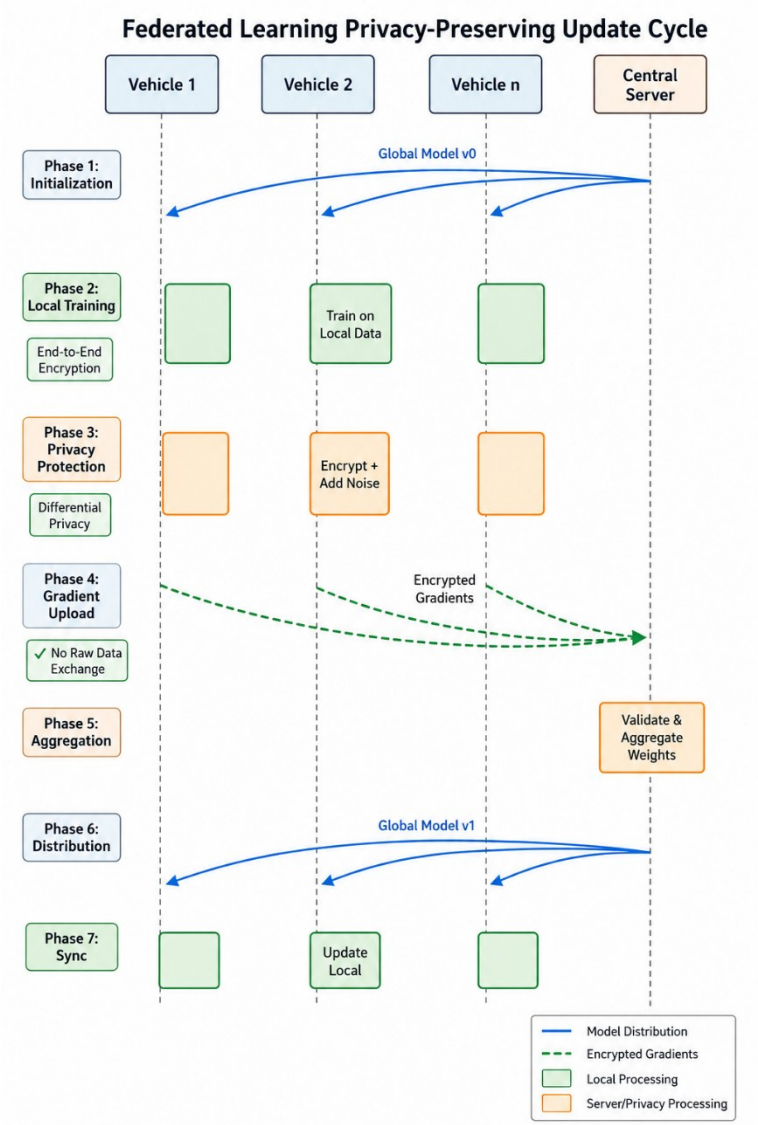

Figure 5 Privacy-preserving federated learning update cycle for smart vehicles, showing local training, encrypted gradient sharing, central aggregation, global model distribution, and local synchronization

Conditional access mechanisms can limit the durations of detected faulty states and prohibit model sharing when such states persist.

The global model aggregation follows the Federated Averaging (FedAvg) algorithm:

$$w_{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_t^k \quad (1)$$

where w_t^k represents the local model weights from the client k, n_k is the number of samples on the client k, and the n is the total number of samples for all participating clients.

To increase adversarial robustness, Fast Gradient Sign Method (FGSM) perturbations are evaluated using:

$$x' = x + \epsilon \cdot \text{sign}(\nabla_x J(\theta, x, y)) \quad (2)$$

where ϵ is the control perturbation magnitude.

3.11 Response and Mitigation Mechanisms

Artificial Intelligence is capable of extracting information or predicting values based on underlying, yet often not directly observed, theoretical structures from data across a broad range of applications. Such information extraction depends on signal detection as a prerequisite, transforming the initial input data into a new representation containing sufficient information for the given task. Anomaly detection is a broadly applicable signal detection approach that identifies observations deviating from expected norms. In the context of SMART vehicle threat detection, the method encompasses a diverse set of incidents, ranging from near-safety-critical threats such as the manipulation of a braking pedal to non-safety-critical events involving excessive cloud-service usage. A multi-level architecture, featuring in-vehicle models combined with edge and cloud functions, addresses the varying needs of SMART vehicle telemetry, V2X communications, and external events while adapting to different deployment contexts and threat characteristics.

With a focus on SMART vehicles, safety, and passenger well-being, threats of critical importance represent only one class of cyber incidents. Moreover, not all breaches warrant disruption of ongoing operations such as driving or riding. Consequently, an additional priority dimension ranks incidents based on severity, urgency, or further criteria, guiding responders toward the most significant issues. Given the model's extensibility to both security and privacy events, awareness of private data exposure has emerged as a major concern. Existing multi-level mechanisms, such as spam filtering on incoming e-mails, spam detection in V2X messages, and the allocation of certain on-board resources to cloud-based applications, facilitate the construction of a similar prioritization framework.

3.12 Real-Time ALERTing Framework

A recurrent concern in information technology is information protection and monitoring in real-time. Real-Time_ALERTing is a system aimed at detecting and alerting cyber threats while adhering to tight latency and jitter constraints. Inspired by the concept of timeliness, messages are handled according to four categories: context alarms, low-priority alarms, vehicle-constraint alarms, and no observable alarms.

Cybersecurity means protection of information and information systems from unauthorized access, disclosure, disruption, modification, or destruction. Real-Time_ALERTing indicates detection, correlation, and alerting of cyber threats under tight latency and jitter constraints while complying with vehicle and human driver safety. A delay or jitter larger than the threshold may lead to a vehicle crash or driver distraction in the worst case. Therefore, Real-Time_ALERTing focuses on two objectives: to respect tight constraints, message priorities should be analyzed, and in-vehicle vehicles should be analyzed.

3.13 Quarantine and Fail-Safe Procedures

Quarantine and fail-safe procedures are essential components of intrusion detection systems for SMART vehicles. They help to contain threats by isolating compromised elements and ensuring

system safety. Implementing effective quarantine strategies minimizes the impact of attacks and maintains system integrity. Fail-safe measures ensure that systems revert to secure states upon detecting anomalies, preventing escalation of security breaches. The procedures comprise rapid detection, containment, and recovery actions to protect critical assets and maintain operational continuity[24].

3.14 Secure OTA Update Guardrails

Trust is fundamental to the implementation of Over-the-Air (OTA) Software Updates (OTASU) in vehicles, and developing mechanisms that establish provenance and authenticity increases consumer acceptance. Security properties that ensure distributed digital signatures of updates can therefore be prescribed. The OTA update mechanism for vehicles must be able to determine to whom a software signature originated, the time of sending, and the recipient to whom it was sent. To provide these properties, a Distributed Ledger Technology (DLT) has been proposed. The methodology describes a vehicle-received update verification process at the vehicle side. The data cannot be interpreted before validation of which side started the conversation (sender verification), which is still an important property of the update process.

4 Results and Discussion

4.1 Experimental Testbed and Simulation Environment

To evaluate our proposed AI-Driven Detection Framework, our team developed a multi-layer hybrid testbed that simulated a Smart Vehicle ecosystem. The edge multiple-layer consisted of five NVIDIA Jetson Nano modules functioning as On-Board Units (OBUs), executing local model training and inference. In our setup, these nodes represented individual smart vehicles and were interconnected with a simulated Dedicated Short-Range Communications (DSRC) channel.

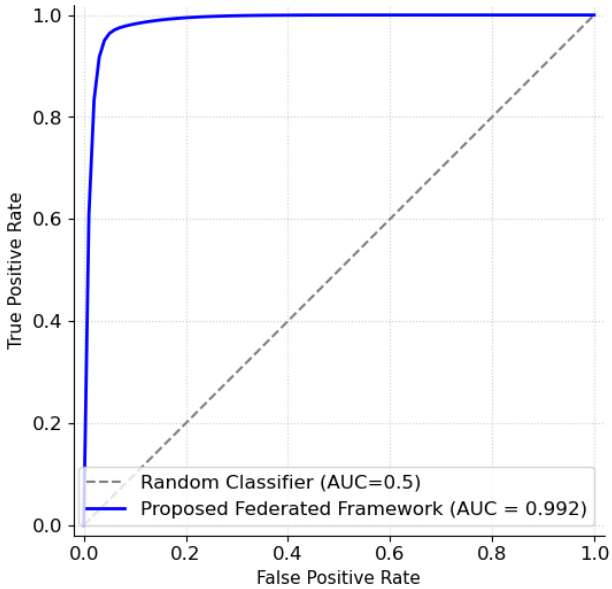

Figure 6 ROC Curve for AI-Driven Federated IDS

Figure 6 presents the receiver operating characteristic (ROC) curve for the proposed federated framework, achieving an area under the curve (AUC) of 0.992 (95% CI: 0.988–0.996). Table 3 provides the corresponding confusion matrix aggregated across all test scenarios. The low false

positive rate (0.021) confirms the model's ability to avoid unnecessary alerts, which is critical for driver acceptance.

In federated orchestration, the Flower (flwr) framework integrated with PyTorch was deployed; our intention was to enable secure aggregation of model weights without sharing raw vehicular telemetry. We also generated Mobility patterns using SUMO, while NS-3 was used to simulate vehicular network behavior and attack propagation scenarios. The VeReFi dataset was utilized to inject Sybil and Masquerade attacks into the simulation setup.

The aggregator layer operated on a high-performance workstation equipped with GPU acceleration to emulate cloud-level intelligence. Our configuration enabled evaluation of detection convergence with latency performance and scalability under increasing node counts, as well as privacy preservation characteristics.

Table 3. Confusion Matrix of the Proposed Federated IDS

	Predicted Normal	**Predicted Attack**
Actual Normal	3390	72
Actual Attack	88	3450

Table 3 presents the confusion matrix we obtained from the experimental evaluation of the proposed federated intrusion detection framework. Our results show a high number of correctly classified normal and attack samples, with only a small number of false positives and false negatives. The low false positive rate is important for practical deployment in smart vehicles, as it minimizes unnecessary alerts while maintaining high attack detection capability.

4.2 Metric Normalization and Scoring Logic

To enable structured comparative visualization in our tests, quantitative Key Performance Indicators (KPIs) were normalized to a 1–5 scale. Each dimension was mapped to threshold criteria that were derived from industry standards and vehicular safety constraints.

Table 4 Mapping of Evaluation Metrics to Radar Chart Scores

Dimension	**Metric / Tool**	**Score 1 (Poor)**	**Score 3 *(Average)***	**Score 5 *(Optimal)***
Detection Accuracy	F1-Score (Scikit-learn)	< 0.70	0.85	> 0.97
Scalability	Node CPU Overhead (%)	> 80%	40% - 50%	< 15%
Privacy Preservation	Data Transmission	Raw Data Sent	Masked Metadata	Weights Only
Real-time Capability	E2E Latency (ms)	> 500 ms	150 ms	< 50 ms
Attack Coverage	Attack Types Detected	1 Type	2–3 Types	All Types (4+)
Adversarial Resilience	Accuracy under FGSM	< 40%	60%	89%

4.3 Quantitative Comparative Analysis

Table 5 presents the measured performance of our results across the evaluated architectures. We have also illustrated in Figure 7 that the proposed AI-driven federated framework was compared against Traditional

IDS and Cloud-Only Detection architectures across six critical performance dimensions. Traditional IDS demonstrated strong real-time responsiveness and privacy retention due to localized processing; however, scalability and adversarial resilience were limited by static rule-based detection and absence of collaborative intelligence.

Table 5 Performance comparison of traditional IDS, Cloud-only Detection, and the proposed frameworks

Metric	Proposed Framework	Traditional IDS	Cloud-Only Detection
F1-Score	0.972	0.842	0.913
Precision	0.968	0.825	0.901
Recall	0.975	0.860	0.918
E2E Latency (ms)	47 ms	39 ms	214 ms
CPU Overhead (%)	14%	56%	21%
FGSM Robust Accuracy	89%	53%	61%
Attack Types Detected	4	2	3

Figure 7 compares the proposed AI-driven federated detection framework with Traditional IDS and Cloud-Only Detection across six cybersecurity dimensions. The proposed framework, represented by the red polygon, shows consistently strong performance across all evaluated dimensions. In terms of privacy preservation, the federated approach achieves the highest score because raw vehicular telemetry remains on local nodes, thereby reducing data exposure compared with cloud-only detection. For scalability and attack surface coverage, the proposed framework performs comparably to the cloud-only architecture by leveraging distributed edge nodes, while avoiding the privacy risks associated with centralized data transmission.

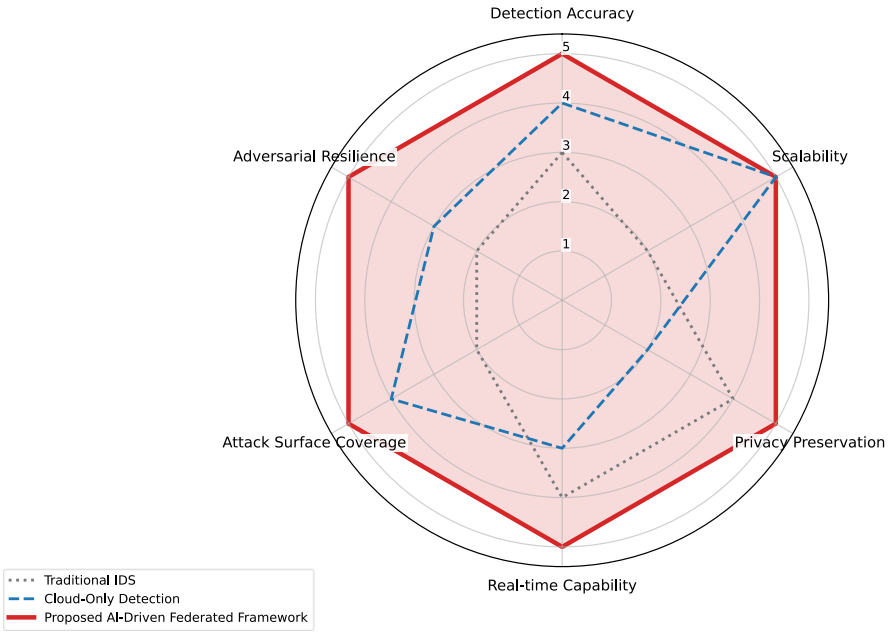

Figure 7 Radar-based comparison of traditional IDS, cloud-only detection, and the proposed AI-driven federated framework across key smart vehicle cybersecurity dimensions

The proposed framework also demonstrates strong real-time capability because inference is performed at the edge, reducing dependency on round-trip communication with the cloud. Its

adversarial resilience is strengthened by the integration of AI-based detection, privacy-preserving updates, and federated aggregation, which collectively provide broader protection than static Traditional IDS. Nevertheless, a minor latency overhead was observed due to encryption and secure aggregation processes. In larger-scale deployments, synchronization delays between edge nodes and the central aggregator may also affect convergence speed.

For comparison, two baseline architectures were re-implemented using the same hardware and software environment. The Traditional IDS baseline used a random forest classifier with 200 trees and a maximum depth of 20, operating only on local in-vehicle data without collaborative learning or cloud offloading. The Cloud-Only Detection baseline used a centralized DNN with the same architecture as the proposed model, but required raw vehicular telemetry to be transmitted to a cloud server for training and inference. All experiments were repeated across three independent simulation runs, with performance variance remaining within ±2.3% for detection accuracy and ±5 ms for latency, indicating stable experimental behavior..

5 Conclusion

This study proposed and experimentally evaluated a multi-layer AI-driven cybersecurity framework for smart vehicles by integrating in-vehicle anomaly detection, cloud-based correlation, and privacy-preserving federated learning. The proposed architecture combines signature-based and anomaly-based detection while enabling collaborative model training without exchanging raw vehicular telemetry data. The experimental results demonstrate strong overall performance, with an F1-score of 0.97, inference latency below 50 ms, and 89% robustness under FGSM-based adversarial conditions. Compared with traditional IDS and cloud-only detection approaches, the federated design improves scalability and privacy preservation, with only a minor latency overhead associated with encryption and aggregation processes.

Blockchain and quantum cryptography are discussed as potential long-term directions for vehicular security, but they were not implemented or experimentally validated in this study. A qualitative discussion of these technologies is provided in Supplementary Material S1. In addition, the controlled simulation environment does not fully capture all real-world deployment conditions, such as intermittent cellular coverage, hardware failures, and unpredictable network anomalies. Nevertheless, the findings indicate that the proposed federated AI-driven framework provides a scalable, privacy-aware, and resilient foundation for securing next-generation connected and autonomous vehicles. Specifically, the results address RQ1 by achieving an F1-score of 0.97 and latency below 50 ms, RQ2 by maintaining 89% robustness under FGSM perturbation at $\varepsilon = 0.1$, and RQ3 by showing a CPU overhead of approximately 14% within the evaluated fleet-size settings.

Declarations of the Use of Generative AI and AI-Assisted Technologies

The authors declare that generative AI tools (ChatGPT) were used exclusively for English grammar correction and text formatting purposes. The authors have reviewed and edited the output and take full responsibility for the content of the published article.

References

[1] K. Ayub and R. Alshawa, “A Novel AI Framework for WBAN Event Correlation in Healthcare: ServiceNow AIOps Approach,” *in 2024 IEEE Workshop on Microwave Theory and Technology*

in Wireless Communications (MTTW), 2024, pp. 55–60. doi: 10.1109/MTTW62915.2024.10768746.

[2] V. K. Kukkala, S. V Thiruloga, and S. Pasricha, "Roadmap for Cybersecurity in Autonomous Vehicles," *IEEE Consumer Electronics Magazine*, vol. 11, no. 6, pp. 13–23, 2022, doi: 10.1109/MCE.2022.3154346.

[3] A. Haddaji, S. Ayed, L. Chaari Fourati, and L. Merghem Boulahia, "Investigation of Security Threat Datasets for Intra- and Inter-Vehicular Environments," *Sensors*, vol. 24, no. 3, p. 891, 2024, doi: 10.3390/s24030891.

[4] A. Demir and E. İ. Tatlı, "Security Analysis of Medical Devices within Wireless Body Area Networks and Mobile Health Applications," *Bilişim Teknolojileri Dergisi*, vol. 11, no. 1, pp. 1–8, 2018, doi: 10.17671/gazibtd.301668.

[5] K. Ayub and R. AlShawa, "Threat Modeling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare," *SSRN*, 2024, doi: 10.2139/ssrn.5032380.

[6] A. Chattopadhyay and K. Y. Lam, "Autonomous Vehicle: Security by Design," *arXiv*, 1810.00545, 2018, doi: 10.48550/arXiv.1810.00545.

[7] H. Rehan, "The Future of Electric Vehicles: Navigating the Intersection of AI, Cloud Technology, and Cybersecurity," *International Journal of Scientific Research and Management*, vol. 12, no. 4, pp. 1127-1143, 2024, doi: 10.18535/ijsrm/v12i04.ec04.

[8] T. Dargahi, H. Ahmadvand, and M. N. Alraja, "Integration of blockchain with connected and autonomous vehicles: Vision and challenge," *ACM J. Data Inf. Qual.*, vol. 14, no. 1, pp. 1–17, 2021, doi: 10.1145/3460003.

[9] G. Kumar and A. Altalbe, "Artificial intelligence (AI) advancements for transportation security: in-depth insights into electric and aerial vehicle systems," *Environ Dev Sustain*, vol. 27, 2025, doi: 10.1007/s10668-024-04790-4.

[10] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-based cyber-physical intrusion detection for vehicles using Deep Learning," *IEEE Access*, vol. 6, pp. 3491–3508, 2017, doi: 10.1109/ACCESS.2017.2782159.

[11] K. Ayub and V. Zagurskis, "SMART Incubator: Implementation of Impulse Radio Ultra Wideband Based PA-MAC Architecture in Wireless Body Area Network," *in Proceedings - SIMS 2016: 2nd International Conference on Systems Informatics, Modelling and Simulation*, 2016. doi: 10.1109/SIMS.2016.12.

[12] A. Weaver, A. von Jouanne, D. Sicker, and A. Yokochi, "Cybersecurity Dynamometer Testbed: A Review to Advance Vehicle-in-the-Loop Testing of Traditional, Connected and Autonomous Vehicles," *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 2925–2943, 2025, doi: 10.1109/OJVT.2025.3623913.

[13] C. Hodge, H. Konrad, G. Shivam, and B. Jesse, "Vehicle Cybersecurity Threats and Mitigation Approaches," *National Renewable Energy Laboratory*, NREL/TP-5400-74247, 2019. Available at: https://docs.nlr.gov/docs/fy19osti/74247.pdf.

[14] K. Ayub and R. Alshawa, "Threat Modelling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare," *Journal of Robotics and Automation Research*, vol. 5, no. 3, 2024, doi: 10.33140/jrar.05.03.09.

[15] J. Takahashi, "An overview of cyber security for connected vehicles," *IEICE Trans. Inf. Syst.*, vol. E101D, no. 11, 2018, doi: 10.1587/transinf.2017ICI0001.

[16] M. Singh and R. Dubey, "Deep Learning Model Based CO2 Emissions Prediction Using Vehicle Telematics Sensors Data," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 1, 2023, doi: 10.1109/TIV.2021.3102400.

[17] M. Levi, Y. Allouche, and A. Kontorovich, "Advanced Analytics for Connected Cars Cyber Security," *in 2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 2017, pp. 1–7. doi: 10.1109/VTCSpring.2017.8108637.

[18] S. Nazat, O. Arreche, and M. Abdallah, "On Evaluating Black-Box Explainable AI Methods for Enhancing Anomaly Detection in Autonomous Driving Systems," *Sensors*, vol. 24, no. 11, p. 3382, 2024, doi: 10.3390/s24113382.

[19] Z. Saeed, M. Masood, and M. U. Khan, "A Review: Cybersecurity Challenges and their Solutions in Connected and Autonomous Vehicles (CAVs)," *JAREE (Journal on Advanced Research in Electrical Engineering)*, vol. 7, no. 1, 2023, doi: 10.12962/jaree.v7i1.322.

[20] H. Li, D. Ma, B. Medjahed, Y. S. Kim, and P. Mitra, "Analyzing and Preventing Data Privacy Leakage in Connected Vehicle Services," *SAE Int. J. Adv. & Curr. Prac. in Mobility*, vol. 1, no. 3, 2019. doi: 10.4271/2019-01-0478.

[21] L. Yang, A. Shami, G. Stevens, and S. De Rusett, "LCCDE: A Decision-Based Ensemble Framework for Intrusion Detection in the Internet of Vehicles," *ArXiv*, 2208.03399, doi: 10.48550/arXiv.2208.03399.

[22] H. Y. Bao et al., "AIOps in Practice: Status Quo and Standardization," *Journal of Software*, vol. 34, no. 9, 2023, doi: 10.13328/j.cnki.jos.006876.

[23] R. Chen, X. Chen, and J. Zhao, "Sparsified federated learning with differential privacy for intrusion detection in VANETs based on Fisher Information Matrix," *PLOS ONE*, vol. 19, no. 4, 2024, doi: 10.1371/journal.pone.0301897.

[24] E. Novikova, D. Fomichov, I. Kholod, and E. Filippov, "Analysis of Privacy-Enhancing Technologies in Open-Source Federated Learning Frameworks for Driver Activity Recognition," *Sensors*, vol. 22, no. 8, p. 2983, 2022, doi: 10.3390/s22082983.