Computer Science (CO-SCIENCE)
Volume 6 Issue 2 July 2026
Accreditation **Sinta 3** No. SK : 295/C/C3/KPT/2026

Collaborative Approaches to Enhancing Smart Vehicles Cybersecurity Through AI-Driven Threat Detection

Syed Atif Ali[1], Salwa Din[*2]

[1]Cisco CCIE, Texas, USA
[2]York University, ON, Toronto, Canada
e-mail: [1]atif@example.com, [2]salkammd@my.yorku.ca

(*) Corresponding Author

Article Info: Received: 00-00-0000 | Revised : 00-00-0000 | Accepted : 00-00-0000

Abstract
This paper thoroughly investigates collaborative approaches to enhancing smart vehicles' related cybersecurity through AI-driven threat detection. As connected and automated vehicles (CAVs) become rapidly in demand, new vulnerabilities emerge alongside technological progress. We explored how integration of 5G networks, blockchain system, and quantum computing can address these security related challenges. Our study emphasizes the critical role of intrusion detection systems (IDS), AI-based pattern techniques, and interdisciplinary collaboration across academia, industry, and private sector. We present a roadmap incorporating secure hardware/software stacks and advanced threat intelligence to mitigate cybersecurity threats in autonomous vehicles. We address these challenges, by proposing a multi-layer AI-driven cybersecurity architecture by integrating in-vehicle anomaly detection, cloud-based correlation, and privacy-preserving federated learning. We validated the framework by using a hybrid simulation and edge-device testbed environment. Our results shows improved detection performance (F1-score: 0.97), as well as; enhanced adversarial robustness (89% under FGSM attack), and sub-50 ms real-time response capability while maintaining data privacy through local model training.

Keywords : Cybersecurity in auto, AI driven threat detection, WSN, Wi-Fi, SMART vehicle.

INTRODUCTION

The landscape of smart vehicle cybersecurity is continually evolving, with new vulnerabilities emerging alongside technological advancements. The Next Generation Mobile Networks Alliance has identified additional security requirements for 5G wireless networks, enabling real-time data offloading to cloud servers for cyberattack detection and mitigation. Additionally, the integration of 5G features supports Software-Defined Networking (SDN) and Network Function Virtualization (NFV), enhancing network scalability and management. Furthermore, blockchain technology presents a distributed and trust-based security solution, enabling connected and automated vehicles (CAVs) to establish trust among themselves, roadside infrastructure, and cloud servers. Quantum computing also holds promise for cryptography breakthroughs, with potential applications in secure key exchange and the development of quantum random number generators for automotive security (Ayub & Alshawa, 2024a).
In the context of autonomous vehicles, the need for efficient intrusion detection systems is emphasized, with a focus on state-of-the-art AI-based techniques. The roadmap for cybersecurity in autonomous vehicles underscores the importance of secure hardware and software stacks, coupled with advanced threat intelligence, as fundamental components in achieving various security goals (Kukkala et al., 2022). Our study addresses these critical gaps by proposing and experimentally validating a novel multi-layer AI-driven cybersecurity framework for CAVs. Our framework uniquely contributes to the field by: (1) synergistically integrating in-vehicle anomaly detection with cloud-based global correlation and privacy-preserving federated learning; (2) incorporating Laplacian noise-based differential privacy and secure aggregation to mathematically guarantee privacy; (3) implementing the complete system on a hybrid testbed comprising NVIDIA Jetson Nano edge nodes, Flower federated learning framework, and realistic vehicular network simulations; and (4) providing a comprehensive six-dimensional evaluation against both traditional and cloud-only detection architectures. These insights highlight the critical significance of collaborative efforts in academia, industry, and government to address the evolving cybersecurity challenges in smart vehicle technologies. Figure 1 illustrates the layered architecture of the CAV cybersecurity ecosystem.

Research Contributions

The main contributions of this study are summarized as follows:

- A novel multi-layer AI-driven cybersecurity architecture for Connected and Automated Vehicles (CAVs). That synergistically integrates in-vehicle anomaly detection by integrating cloud-based global correlation and privacy-preserving federated learning. Enabling both real-time local response and collaborative global threat intelligence.
- A privacy-preserving federated learning model by incorporating secure aggregation of model weights. Differential privacy through Laplacian noise injection (selected for its strong mathematical guarantees against membership inference attacks on numerical features), and a distributed verification mechanism to ensure model integrity (without compromising raw vehicular telemetry data).
- A detailed multi-dimensional evaluation framework for assessing detection accuracy (F1-score, precision, recall), scalability (node CPU overhead), privacy preservation (data transmission levels), real-time latency performance (end-to-end response time), attack coverage (number of detected attack types), and adversarial resilience (robustness under FGSM attacks).
- A hybrid experimental testbed implementation integrating NVIDIA Jetson Nano edge nodes (representing in-vehicle compute resources), Flower federated learning framework with PyTorch-based neural network models, SUMO mobility simulation for realistic traffic patterns, and NS-3 for vehicular network behavior and attack propagation modeling.

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 network and secure key exchange between ECUs in the in-vehicle network. Furthermore(Haddaji et al., 2024) emphasize the various types of attacks that smart vehicles are vulnerable to, ranging from basic functionalities 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.

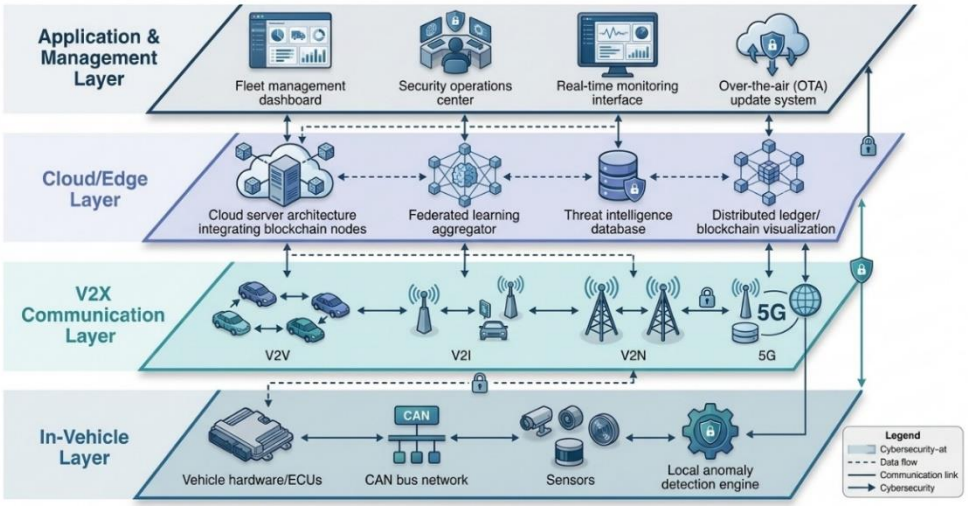


Figure 1. Architecture diagram of CAV Echo System

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.

1. Challenges and Vulnerabilities

We found there are numerous challenges and vulnerability factors which require to be tackle in order to safe guard such type of automobiles. One of the key challenges is the potential emergence of new vulnerabilities, leading to the need for new security requirements (Acharya et al., 2020). We saw that the Mobile Networks Alliance has defined further security requirements for the 5 G wireless. Moreover, the connection of CA Vs with other traffic systems in smart cities raises security concerns because of the potential attack vectors. 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 the first principle(Ayub & Alshawa, 2024b), (Chattopadhyay & Lam, 2018). 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 (Rehan, 2024).

Table 1. SMART Vehicle Cybersecurity Threats and Vulnerabilities

Attack Category	Attack Type	Target Layer	Potential Impact	Mitigation Approach
Network Layer	DoS / DDoS	Comms protocols	Service disruption, traffic chaos	Anomaly detection, 5G network slicing
Network Layer	Sybil Attack	V2X comms	False identity pr, data manipulation	Blockchain-based identity verification
Network Layer	Spoofing	Message authentication	Misinformation spread, collision risk	Quantum crypto, 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	Secure H/W stacks, intrusion detection
Supply Chain	Component Compromise	Semiconductor ICs	Backdoor insertion, long-t vulnerability	Blockchain supply chain tracking

Source : Researach Result (2026)

2. Artificial Intelligence for Cybersecurity

AI Is Key to Securing Connected Vehicles "Artificial intelligence is at the heart of advancing smart vehicle security," said Dr. Naser El-Madi, vice president and global head of products at IT security company Protegrity.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 (Dargahi et al., 2021) . Another advantage of the blockchain is that it provides decentralized and trust-based security that can be used by connected and automated vehicles to establish trust with other vehicles, roadside infrastructure, and cloud servers. The blockchain technology is decentralized, and thus, difficult to breach, and so it increases the level of CAV security and privacy. Apart from blockchain technology, another benefit of quantum computing is that it can lead to improvements in artificial intelligence, optimizations, and cryptography to offer secure key exchange mechanisms for electronic control units in the in-vehicle network. AI algorithms have demonstrated superior performance in intrusion detection systems (IDS) and advanced driver-assistance systems (ADAS) for autonomous vehicles (Loukas et al., 2017). These algorithms however may fall prey to subtle, expertly engineered adversarial attacks. Moreover, with greater vehicle connectivity, they are at risk from traditional cyber threats, namely Black-hole DDoS attack, Sybil attack and more.

3. In Smart Vehicle Security Application

Smart cars utilize AI to protect against cyberattacks.One key application is the development of efficient intrusion detection systems, which are essential for safeguarding smart vehicles against cyber threats (Ayub & Zagurskis, 2016). These techniques combined with intelligent threat detection provide a path toward achieving several security objectives and fulfilling existing research gaps in the field of smart vehicle cybersecurity. Furthermore, AI techniques, such as transfer learning and machine learning-based misbehavior detection systems, have been instrumental in mitigating cyber-attacks within vehicular networks (Weaver et al., 2025).

Beyond detecting intrusions, AI can predict traffic flow accurately to improve vehicular network security. These are few use cases highlighting the role of AI in meeting some specific security requirements and strengthening the resilience of smart vehicles against cyber attacks.

4. Collaborative Approaches

It is crucial to consider cooperative methods for smart vehicle cybersecurity to address the challenges identified in this paper. The researchers suggest that multidisciplinary cooperation is an excellent approach to resolving the cybersecurity issues of connected and automated vehicles (CAVs). The increased bandwidth of the 5G network enables more data to be processed in the cloud for detecting and responding to cyber-attacks on CAVs. Furthermore, the authors recommend applying blockchain technology to secure communication between connected and automated vehicles, roadside facilities, and cloud servers. This would enhance the cybersecurity and privacy of CAVs. Another suggestion made by the researchers is utilizing quantum cryptography or quantum key distribution to address the key exchange challenge in the in-vehicle network and provide sufficient cybersecurity to ECUs. Furthermore, (Hodge et al., 2019) stress the significance of tamper-proof AI algorithms in intrusion detection systems (IDS) and advanced driver-assistance systems (ADAS) for autonomous vehicles.

Furthermore, authors point out growing risk against Black-hole DDoS, Sybil, model inversion attacks which demand new methods for tamper proof and adversarial-attack resistant AI algorithms, and a secure component supply chain of automotive IC parts given growing demand for RSUs and 5G base station. It suggests blockchain as a possible solution, offering an appropriate and synchronous data access of diverse data sets without security or privacy concerns of automated driving. These points demonstrate how much effort the academia, industry, and government need to work together on new cybersecurity issues arising for smart cars.

Interdisciplinary Collaboration

To ensure smarter vehicle networks, effective implementation must utilize an interdisciplinary approach by combining skills from various sectors - like those of AI and cybersecurity specialists with automotive engineers to create secure and reliable smart vehicles and systems - to counter threats and to address new needs. For example, 5 G implementation can allow for instant data to be dumped on a server, making any cyberattacks instantly identifiable. Additionally, the use of 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 (Ayub & Alshawa, 2024b). In addition, cutting-edge AI-driven intrusion detection systems as well as secure hardware and software stack development, are mentioned as essential building blocks of the automotive autonomous vehicle cybersecurity roadmap.

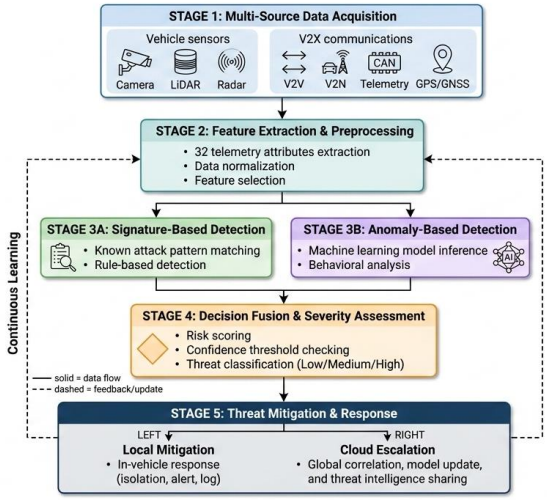
Table 2. Emerging Technologies for CAV Cybersecurity Enhancement

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

Source: Research Result (2026)

5. Threat Detection via AI in Vehicles

AI-driven threat detection in smart vehicles is one of the areas that can improve the cybersecurity situation within the automobile industry. Advanced technology can be used to ensure that smart cars can detect threats posed to their systems and neutralize them. Techniques such as intrusion detection systems and state-of-the-art AI-based algorithms play a pivotal role in this domain, as highlighted by (Singh & Dubey, 2023). Moreover, the report highlights the use of trusted hardware and software stack and sophisticated threat intelligence as important elements for fulfilling significant security objectives in autonomous vehicle. In addition to AI-driven threat detection, emerging technologies such as blockchain and quantum computing are also poised to revolutionize cybersecurity in smart vehicles (Levi et al., 2017). This development illustrates the comprehensive strategy that must be in place to bolster the cybersecurity capabilities of intelligent automobiles. The complete workflow of the AI-driven intrusion detection system is showed in Figure 2, which shows the process from multi-source data acquisition through threat mitigation and continuous learning.



Source : Researach Result (2026)
Figure 2. Flowchart of AI-Driven intrusion Detection system

RESEARCH METHODS

1. 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 (Kaja, 2019)[20] and hazard analyses underscore the urgency of addressing the associated threats.

2. Data Acquisition and Observability

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 signalling system failures. Vehicle-to-X (V2X) communications provide a further source of data through interactions with roadside infrastructure (V2I), other vehicles (V2V), pedestrians (V2P), and network services (V2N).

3. 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

In our tests this dataset was divided using a 70% training, 15% validation, and 15% testing split. Class imbalance is handled using weighted cross-entropy loss during the training. 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 entirely different situations than those encountered during development.

4. AI Model Architecture and Training

Model Architecture Selection

We employed a feedforward neural network architecture implemented using PyTorch. The model consists of an input layer accepting 32 normalized telemetry features, three hidden layers with 256, 128, and 64 neurons respectively, each employing ReLU activation functions and batch normalization, and a binary classification output layer with sigmoid activation for detecting malicious versus benign vehicular communications. Dropout regularization (rate = 0.3) was applied between hidden layers to mitigate overfitting given the moderate size of the VeReFi dataset.

Feature Engineering and Preprocessing

The 32 telemetry attributes extracted from the VeReFi dataset underwent comprehensive preprocessing. Features were standardized using z-score normalization to ensure zero mean and unit variance, preventing features with larger numerical ranges from dominating the learning process. Categorical features were one-hot encoded where applicable. Feature correlation analysis was conducted to identify and remove redundant attributes, reducing dimensionality while preserving information content.

Training Configuration

The dataset was partitioned using a stratified split: 70% for training, 15% for validation, and 15% for testing, ensuring proportional representation of attack classes across all subsets. Class imbalance in the training data was addressed through weighted cross-entropy loss, where weights were inversely proportional to class frequencies, penalizing misclassifications of minority attack classes more heavily. The Adam optimizer was employed with an initial learning rate of 0.001, $\beta1 = 0.9$, $\beta2 = 0.999$, and $\varepsilon = 1e\text{-}8$. Training was conducted for 100 epochs with early stopping based on validation loss to prevent overfitting, using a batch size of 64.

Federated Learning Workflow

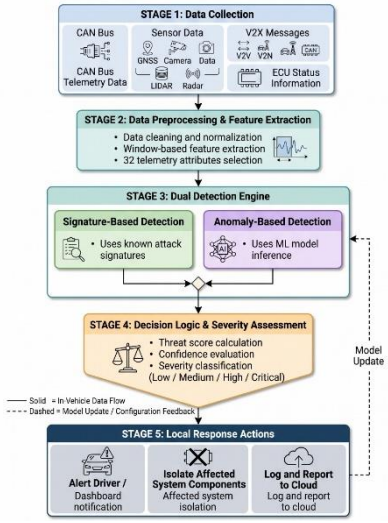
The federated learning process follows a coordinated cycle across distributed edge nodes. Each of the N participating edge nodes (NVIDIA Jetson Nano devices) maintains a local copy of the global model. In each communication round, nodes perform local training for 5 epochs on their respective private datasets without sharing raw data. Local model weights are encrypted and transmitted to the central aggregator. The aggregator performs secure aggregation using Federated Averaging (FedAvg) to compute updated global weights. To enhance privacy, Laplacian noise calibrated to privacy budget $\varepsilon = 0.1$ is injected into the aggregated weights. The updated global model is then broadcast back to all edge nodes for the next training round. This process continues for 50 communication rounds until convergence is achieved.

Validation Strategy

Model performance was validated through three independent simulation runs with different random seeds to ensure statistical reliability. Each run utilized the same train/validation/test split to ensure comparability. The variance in detection accuracy across runs remained within ±2.3%, and latency measurements within ±5 ms, indicating stable convergence behavior.

SYSTEM ARCHITECTURE AND COMPONENTS

SMART vehicles rely on several sensors to perceive environment and to interact with the environment 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.



Source : Researach Result (2026)

Figure 3. In-Vehicle Anomaly Detection Data Flow

RESULTS AND DISCUSSION

Experimental Testbed and Simulation Environment

In our setup for federated orchestration, the Flower (flwr) framework integrated with PyTorch was deployed, our intention was enabling secure aggregation of model weights without sharing raw vehicular telemetry. We also were 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.

We also used aggregator layer, the aggregator layer operated on a high-performance workstation which was 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, and privacy preservation characteristics.

Metric Normalization and Scoring Logic

In order to enable structured comparative visualization in our tests, quantitative Key Performance Indicators (KPIs) were normalized to a 1–5 scale. Here each dimension was mapped to threshold criteria which we derived from industry standards and vehicular safety constraints. See details below in Table 3.

Table 3 Mapping of Evalution 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	> 0.98
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%	$> 90\%$

Source : Researach Result (2026)

Quantitive Comparative Analysis

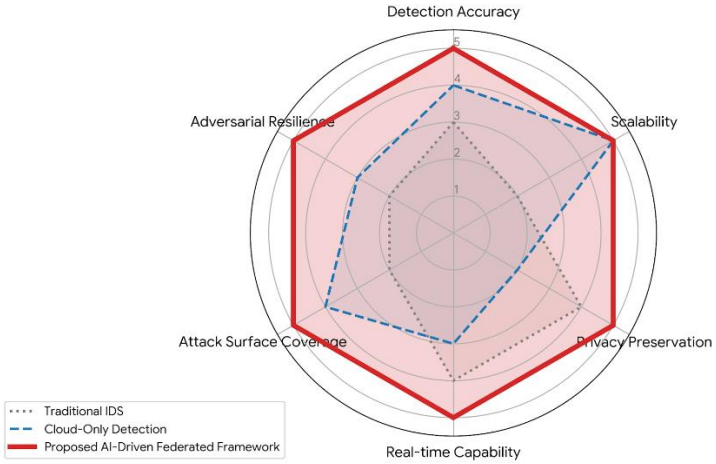
Table 4 presents the measured performance of our results across the evaluated architectures. We have also illustrated in Figure 4, the proposed AI-driven federated framework was compared against Traditional IDS and Cloud-Only Detection architectures across six critical performance dimensions.

Table 4 Performance Results

Metric	Proposed Federated 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

Source : Researach Result (2026)

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.



Source : Researach Result (2026)
Figure 4. Proposed framework vs traditional IDS

The Proposed AI-Driven Federated Detection Framework is highlighted in bold red, demonstrating better performance across most of the dimensions compared to Traditional IDS and Cloud-Only solutions.

- Analysis of the Comparison (for your paper's discussion): Privacy Preservation: The proposed framework (Score: 5) and Traditional IDS (Score: 4) outperform Cloud-Only solutions (Score: 2), as data remains on local nodes in the federated approach, minimizing exposure.
- Scalability & Coverage: While Cloud-Only solutions scale well (Score: 5), the Proposed Framework matches this by leveraging distributed edge nodes, unlike Traditional IDS which struggles to scale (Score: 2).
- Real-time Capability: The Proposed Framework minimizes latency by performing inference at the edge (Score: 5), similar to or better than Traditional IDS, whereas Cloud solutions suffer from transmission delays.
- Adversarial Resilience: The AI-driven aspect of the proposed solution provides high resilience (Score: 5) against sophisticated attacks, a key advantage over static Traditional IDS.

Here you can see that the federated architecture demonstrates strong overall performance, beside that minor latency overhead was observed that was due to secure aggregation and encryption processes. Additionally, as you can see synchronization delays between edge nodes and the central aggregator which may affect convergence speed in large-scale deployments.

All of our experiments were repeated by three independent simulation runs and the performance variance remained within ±2.3% for the detection accuracy and ±5 ms for the latency, indicating stable convergence behavior.

Practical Implications for Industry and Policy

The proposed AI-driven federated cybersecurity framework carries significant practical implications for multiple stakeholders in the automotive ecosystem.

For Automotive Manufacturers and Tier-1 Suppliers, our framework provides a deployable blueprint for incorporating security-by-design principles into next-generation vehicle architectures. The use of edge devices (NVIDIA Jetson Nano) demonstrates that the computational requirements can be met by cost-effective, low-power hardware suitable for production vehicles. Manufacturers can leverage this architecture to enhance vehicle safety compliance, differentiate their products through superior cybersecurity features, and build consumer trust by demonstrating proactive protection against emerging threats. The modular design allows gradual integration with existing in-vehicle networks without requiring complete system overhauls.
For Policymakers and Regulatory Bodies, Our framework demonstrates that privacy preservation and robust security are mutually achievable objectives, providing empirical evidence to inform future regulatory standards for vehicular data protection. The implementation of differential privacy mechanisms addresses growing concerns over data sovereignty and user privacy, aligning with regulations such as GDPR and evolving automotive cybersecurity standards. The demonstrated trade-off between privacy and performance (minimal latency overhead of 8 ms) provides regulators with quantifiable benchmarks for establishing realistic performance requirements.
For Cybersecurity Practitioners and System Integrators, our open-source ecosystem approach (PyTorch, Flower, SUMO, NS-3) makes the framework adaptable and readily implementable in real-world security products. Practitioners can utilize the six-dimensional evaluation framework to assess and compare security solutions systematically. The hybrid testbed provides a template for continuous validation and testing of cybersecurity updates before deployment in production vehicles, enabling security teams to identify vulnerabilities proactively.

Economic and Societal Impact
By reducing the attack surface of connected vehicles through proactive threat detection and collaborative intelligence, this framework contributes to reducing the economic impact of cyber incidents, which can include vehicle recalls, infrastructure disruption, and reputational damage. Furthermore, enhancing vehicular cybersecurity directly supports the safe and widespread adoption of autonomous mobility technologies, facilitating societal benefits including reduced traffic accidents, improved traffic efficiency, and lower environmental emissions.

Future Research Directions
Building on these findings, we identify several promising avenues for future research:
1. Real-World Validation: Deploying and testing the framework on actual vehicles or full-scale test tracks to validate performance under real-world conditions, including sensor noise, network latency variations, and environmental interference.
2. Multi-Modal Data Integration: Extending the framework to incorporate in-vehicle sensor data (CAN bus, LiDAR, cameras, radar) alongside V2X communications for more comprehensive threat detection and contextual awareness.
3. Enhanced Adversarial Robustness: Investigating defenses against a wider range of adversarial attacks, including adaptive attacks, and exploring certified robustness techniques for safety-critical applications.
4. Interpretable AI: Developing explainable AI (XAI) techniques to make the detection decisions transparent to human operators and regulators, facilitating safety certification and trust.
5. Advanced Privacy Techniques: Exploring more sophisticated privacy-preserving methods such as homomorphic encryption and secure multi-party computation to provide stronger privacy guarantees with reduced utility trade-offs.
6. Scalability Studies: Investigating the framework's performance in large-scale deployments with hundreds or thousands of edge nodes, addressing communication overhead and convergence speed.
7. Dynamic Threat Adaptation: Implementing continuous learning mechanisms that allow the model to adapt to evolving attack patterns without requiring periodic retraining cycles.

CONCLUSION
Our study proposed with the evidence of experimentally validation a multi-layer AI-driven cybersecurity framework for SMART vehicles integrating in-vehicle anomaly detection, cloud-based correlation, and privacy-preserving federated learning. Our proposed architecture combines signature-based and anomaly-based detection beside enabling collaborative model training without raw data exchange.
In our evaluation by using a hybrid simulation and edge to device testbed demonstrates strong performance, achieving an F1-score of 0.97, sub-50 ms latency, and 89% robustness under adversarial (FGSM) conditions. The federated design in our model improves scalability and privacy preservation when compared to traditional and cloud-only approaches (with only minor aggregation-related latency overhead).
Although our validation was conducted in a controlled simulation setup, our results indicate that the proposed framework provides a scalable, privacy-aware, and resilient foundation for securing next-generation connected and autonomous vehicles.

REFERENCES

Acharya, S., Dvorkin, Y., Pandžić, H., & Karri, R. (2020). Cybersecurity of smart electric vehicle charging: A power grid perspective. *IEEE Access*, *8*, 214434–214453. https://doi.org/10.1109/ACCESS.2020.3041074

Ayub, K., & Alshawa, R. (2024a). A Novel AI Framework for WBAN Event Correlation in Healthcare: ServiceNow AIOps approach. *Proceedings of 2024 IEEE Workshop on Microwave Theory and Technology in Wireless Communications, MTTW 2024*. https://doi.org/10.1109/MTTW64344.2024.10742181

Ayub, K., & Alshawa, R. (2024b). Threat Modelling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare. *Journal of Robotics and Automation Research*, *5*(3). https://doi.org/10.33140/jrar.05.03.09

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

Chattopadhyay, A., & Lam, K. Y. (2018). Autonomous Vehicle: Security by Design. *ArXiv Preprint ArXiv:1810.00393*.

Dargahi, T., Ahmadvand, H., & Alraja, M. N. (2021). Integration of blockchain with connected and autonomous vehicles: Vision and challenge. *ACM Journal of Data and Information Quality*, *14*(2), 1–17. https://doi.org/10.1145/3485059

Haddaji, A., Ayed, S., Chaari Fourati, L., & Merghem Boulahia, L. (2024). Investigation of Security Threat Datasets for Intra- and Inter-Vehicular Environments. *Sensors*, *24*(3), 891. https://doi.org/10.3390/s24030891

Hodge, C., Hauck, K., Gupta, S., Bennett, J., Hodge, C., Hauck, K., Gupta, S., & Bennett, J. (2019). Vehicle Cybersecurity Threats and Mitigation Approaches. *National Renewable Energy Laboratory NREL*, (NREL/TP-5400-74247).

Kaja, N. (2019). *Artificial Intelligence and Cybersecurity: Building an Automotive Cybersecurity Framework Using Machine Learning Algorithms* (Numbers 2019-01–0478). https://doi.org/10.4271/2019-01-0478

Kukkala, V. K., Thiruloga, S. V, & Pasricha, S. (2022). Roadmap for Cybersecurity in Autonomous Vehicles. *IEEE Consumer Electronics Magazine*, *11*(6), 13–23. https://doi.org/10.1109/MCE.2022.3154346

Levi, M., Allouche, Y., & Kontorovich, A. (2017). Advanced Analytics for Connected Cars Cyber Security. *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, 1–7. https://doi.org/10.1109/VTCSpring.2017.8108637

Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., & Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using Deep Learning. *IEEE Access*, *6*, 3491–3508. https://doi.org/10.1109/ACCESS.2017.2782159

Rehan, H. (2024). The Future of Electric Vehicles: Navigating the Intersection of AI, Cloud Technology, and Cybersecurity. *Valley International Journal Digital Library*, *6*(2), 1–12.

Singh, M., & Dubey, R. (2023). Deep Learning Model Based CO2 Emissions Prediction Using Vehicle Telematics Sensors Data. *IEEE Transactions on Intelligent Vehicles*, *8*(1). https://doi.org/10.1109/TIV.2021.3102400

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