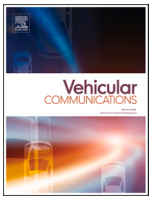
Vehicular Communications 59 (2026) 101024

Contents lists available at ScienceDirect

Vehicular Communications

journal homepage: www.elsevier.com/locate/vehcom



Securing automotive data flow: A survey of telematics security across intra-vehicle, V2X, and cloud layers

Junjie Wu [a], Benjamin C. M. Fung [a,*], Natalia Stakhanova [b], Faiyaz Khan [b], Hanbo Yu [a]

[a] School of Information Studies, McGill University, Canada
[b] Department of Computer Science, University of Saskatchewan, Canada

ARTICLE INFO

Keywords:
Automotive cybersecurity
Telematics
V2X
Intra-vehicle network
Cloud security
Intrusion detection systems (IDS)

ABSTRACT

This survey systematically analyzes 77 studies on automotive telematics security, examining solutions across Intra-Vehicle Networks, Vehicle-to-Everything (V2X) communications, and Cloud/IoT (Internet of Things) integration. Through comparison with 13 prior surveys, we identify a critical research gap: existing literature predominantly addresses these layers in isolation, failing to adequately secure data flows across architectural boundaries. Our cross-layer analysis reveals that hybrid intrusion detection systems achieve up to 99.5% accuracy against CAN bus attacks, federated learning frameworks attain 99% DDoS detection while preserving privacy, and secure interface mechanisms enable sub-100 μs latency transitions with 52% reduced overhead for over-the-air updates. We closely examine intrusion detection systems, secure communication protocols, privacy protection techniques, and attack resilience strategies, identifying both the strengths and limitations of current approaches. Additionally, we evaluate how emerging technologies such as artificial intelligence and machine learning can improve the resilience of telematics systems against advanced cyber threats. Our findings indicate that securing automotive data requires a unified, cross-layer cybersecurity strategy to ensure data integrity, confidentiality, and availability, guiding future research in this vital area.

1. Introduction

In 2024, security researchers discovered a severe vulnerability in Subaru's Starlink connected vehicle service. This vulnerability allowed attackers to remotely control vehicles across multiple countries using only minimal information-a license plate or basic owner details such as a last name or Email address [1]. This breach allowed unauthorized control and exposed a year of precise location data, prompting a rapid patch from Subaru. In contrast to the 2015 Jeep Cherokee hack, which involved remotely manipulating critical functions including braking and steering [2], the Subaru incident required only publicly available data and not physical access or advanced tools. This evolution shows how attackers now exploit the growing digital footprint of connected vehicles. These modern vulnerabilities pose significant risks to safety and privacy, requiring urgent advances in cybersecurity.

Telematics security is crucial for protecting modern vehicles, which integrate telecommunications and informatics to deliver advanced features. These include autonomous driving capabilities, remote diagnostics, and connectivity to Intelligent Transportation Systems (ITS). These capabilities are achieved through a layered architecture that includes Intra-Vehicle Networks, also known as in-vehicle networks (IVNs); V2X systems for external connectivity with other vehicles and infrastructure; and Cloud/IoT Integration for services such as over-the-air (OTA) upgrades. The automotive sector is rapidly transforming due to this increase in connectivity and automation, with projections that 95% of new cars will be connected by 2030 [3]. Innovations in collision avoidance, traffic optimization, and predictive maintenance all depend on the reliable exchange of data across these architectural layers.

This connectivity and data exchange significantly increase the vehicle's attack surface. Vulnerabilities arise from the data flows traversing the interfaces between the Intra-Vehicle, V2X, and Cloud/IoT layers. Wireless communication channels, external cloud connections, and internal network gateways serve as potential entry points for malicious actors. The inherent interdependence of these layers means that a security breach in one domain, such as a compromised cloud service initiating an OTA update, can directly compromise safety-critical ECUs (Electronic Control Unit) within the network. Similarly, externally received V2X messages, without validation at the interfaces, could manipulate

* Corresponding author.
E-mail address: ben.fung@mcgill.ca (B.C.M. Fung).

https://doi.org/10.1016/j.vehcom.2026.101024
Received 12 July 2025; Received in revised form 27 January 2026; Accepted 19 March 2026
Available online 23 March 2026

Table 1
Coverage of telematics security dimensions in recent surveys (●: Complete; ◐: Partial; ○: None).

Study	Year	Layer Coverage				Security Dimension		
		In-vehicle	V2X	Cloud/IoT	Cross-layer	Data-flow	Attacks	Defences
Luo et al. [33]	2018	●	○	○	○	○	●	◐
Wu et al. [68]	2020	●	○	○	○	○	●	●
Sedar et al. [49]	2023	◐	●	○	○	○	●	○
Anwar et al. [3]	2023	●	○	○	○	○	●	◐
Hossain et al. [20]	2023	●	●	○	◐	○	●	●
Rao et al. [45]	2023	○	●	●	◐	○	◐	◐
Taslimasa et al. [55]	2023	●	●	◐	◐	○	●	●
Gul & Ertam [15]	2024	●	○	○	○	○	●	●
Kifor et al. [25]	2024	●	●	○	◐	○	◐	◐
Pali et al. [41]	2024	○	●	●	◐	○	◐	○
Rishiwal et al. [47]	2024	○	●	●	◐	○	○	◐
Zhang et al. [76]	2024	●	○	○	○	○	◐	●
Farsimadan et al. [11]	2025	○	●	○	○	○	●	◐
Our survey	2026	●	●	●	●	●	●	●

internal vehicle controls. This potential for threat propagation across architectural boundaries creates systemic risks to a vehicle's safety, privacy, and reliability. Therefore, this survey provides a focused analysis of the security challenges and solutions relevant to data flow within each telematics layer and, crucially, at the interfaces connecting them.

Despite the clear importance of securing these interconnected data pathways, existing research often addresses telematics security in a fragmented manner. Connected vehicles are vulnerable to several threats, including faked CAN messages that impair braking systems, intercepted V2X communications that violate privacy, and modified OTA updates that undermine system integrity [2]. However, as highlighted by Wang et al. [4], systematic cybersecurity risk assessment integrating Intra-Vehicle, V2X, and Cloud/IoT perspectives is rarely proposed. Prior surveys frequently concentrate on specific layers in isolation, such as intra-vehicle security [5,6] or V2X communications [7,8], without a dedicated, in-depth analysis of the security of data as it moves across these architectural boundaries and their interfaces. This fragmentation reveals a major gap: there is no comprehensive understanding of how to keep data flowing safely across the entire telematics ecosystem, where weaknesses can propagate and compromise vehicle safety and reliability.

This paper aims to bridge this gap. As demonstrated in Table 1, existing surveys predominantly address individual layers in isolation; notably, none of these works provides comprehensive coverage of all three telematics layers while also examining data flow security across their interconnections. Unlike prior surveys that focus on specific domains, this work uniquely synthesizes security perspectives across the entire telematics ecosystem. Our primary contributions are:

1. **First comprehensive cross-layer analysis:** We provide the first systematic analysis of security challenges and solutions targeting data flow integrity, confidentiality, and availability across all three core telematics layers, namely, Intra-Vehicle Network, V2X Communication, and Cloud/IoT Integration, within a unified framework.
2. **Novel interface-centric security evaluation:** We present the first dedicated evaluation of security mechanisms and vulnerabilities at the interfaces interconnecting these layers, explicitly addressing cross-layer threat propagation pathways that prior surveys have overlooked.
3. **AI/ML integration assessment:** We offer a comprehensive survey of the application and efficacy of emerging AI/ML technologies in enhancing data flow security throughout the telematics stack, evaluating their deployment from internal networks through external communications to cloud interactions.

This survey focuses on security aspects of data transfer and inter-layer transitions. While relevant protocols (e.g., CAN, C-V2X) and components (e.g., ECUs) provide context, we do not perform an in-depth analysis of the protocols themselves or of isolated hardware security. This work presents a cross-layer architecture by integrating recent advances and methodically analyzing the data journey. By consolidating previously disparate studies, we offer an extensive perspective on vulnerabilities and countermeasures. Our analysis covers hybrid Intrusion Detection Systems (IDS) for internal networks, federated learning for V2X privacy, and secure gateways for interface transitions.

The remainder of this paper is structured as follows: Section 2 further elaborates on the identified research gap by critically examining existing surveys. Section 3 introduces the telematics layers in detail. Section 4 presents our comprehensive analysis of data flow security solutions. Finally, Section 5 discusses the implications of our findings, outlines limitations, and proposes future research directions.

2. Gap identification

The automotive industry's rapid shift towards connectivity and automation introduces complexity into vehicle electrical/electronic (E/E) architectures [5]. While enabling advanced features such as autonomous driving and ITS, this integration of numerous ECUs, sensors, and communication interfaces significantly expands the potential attack surface. Vulnerabilities are no longer limited to physical access; remote exploitation via wireless interfaces poses a verified threat, exemplified by the 2021 breach of the Tesla Model X keyless entry system due to Bluetooth vulnerabilities [9]. Adversaries can target external communication channels or pivot to internal networks, potentially compromising vehicle safety and user privacy [2]. As a result, researchers and engineers are actively developing comprehensive cybersecurity frameworks, standards, and technologies. Yet, understanding how different system layers function together remains challenging.

Central to these advanced functionalities is the reliance on real-time data analytics, processing information from diverse sources including internal sensors, V2X communications, and cloud systems [7]. Applications such as collision avoidance or optimized traffic flow depend fundamentally on the timely and trustworthy exchange of these data. However, existing security assessments often fail to adequately address the

risks of data flowing across different architectural layers-for instance, from an internal sensor, through a gateway, via V2X, and finally to the cloud. A compromised data stream at any point in this chain could lead to catastrophic failures, from incorrect vehicle maneuvers to manipulated traffic infrastructure. However, the literature still lacks a thorough analysis of data flow security across the entire telematics ecosystem, leaving the risks that span intra-vehicle, V2X, and Cloud/IoT layers poorly understood [4,10]. Much of the current research investigates security aspects within individual domains, without fully capturing the risks inherent in data transitions between them.

Current studies often emphasize isolated components or communication channels, overlooking their essential interdependencies. For instance, Kifor [5] provides a broad overview of cybersecurity frameworks and testing methodologies but does not specifically address their application to securing data flow across telematics layers. Similarly, Soundarapandiyan et al. [7] emphasize the importance of real-time analytics for ITS without exploring the security implications of data movement within the system. Wang et al. [4] further highlight this fragmentation, observing that "most studies focus on risk rating methods, but systematic cybersecurity risk assessment for automobiles is rarely proposed." This fragmented approach fails to tackle the unique security challenges posed by diverse data flows in the telematics ecosystem, where a breach in one layer (e.g., intra-vehicle network) can cascade to others, e.g., V2X or Cloud/IoT.

Recent surveys further illustrate this fragmentation, as summarized in Table 1. Studies focusing on intra-vehicle networks, such as [6,10,11], and the comprehensive survey by Wu et al. [12] on IVN IDS, examine vulnerabilities in protocols such as CAN, LIN, and T-Box systems, offering insights into internal threats and countermeasures. However, they rarely consider how these internal networks interact with external systems such as V2X or Cloud/IoT. Conversely, research on V2X and external communications focuses on external threats, including blockchain-based security and human-centric privacy [13–17]. However, this work often neglects the foundational intra-vehicle layer. Rao et al. [13], for instance, explore application of blockchain for IoT-enabled V2X communications, which addresses external data exchange security but overlooks intra-vehicle network vulnerabilities. Taslimasa et al. [8] attempt a broader scope by surveying IoV security, covering intra- and inter-vehicle communications, but still fall short of fully integrating Cloud/IoT layers. General frameworks, such as those by Kifor [5] and Sedar et al. [18], offer overarching models or focus on specific technologies (e.g., V2X communication protocols), yet lack cross-layer integration.

This research addresses this critical gap by providing a comprehensive analysis of data flow security across intra-vehicle networks, V2X communication, and Cloud/IoT integration. Unlike prior studies, it explicitly examines the interconnections among these layers, evaluating the effectiveness of existing and emerging security solutions across channels and interfaces. For instance, while Taslimasa et al. [8] highlight intra- and inter-vehicle threats, this study extends the analysis to Cloud/IoT interactions, ensuring a complete view. The study also explores how machine learning (ML) and artificial intelligence (AI) can improve data flow security through anomaly detection, intrusion detection, and proactive threat prediction. Our integrated approach aims to directly improve the safety, reliability, and trustworthiness of connected vehicles. To analyze and secure data flow effectively, a clear understanding of these layers and their interconnections is essential. The next section, Introduction to Telematics Layers, provides this foundation by detailing the structure and function of these interconnected layers.

3. Telematics layers: foundations for security analysis

Modern automotive telematics systems integrate three interconnected layers-Intra-Vehicle Network, V2X Communication, and Cloud/IoT Integration-to enable advanced functionalities such as autonomous driving, real-time diagnostics, and smart city connectivity. The *Intra-Vehicle Network* layer coordinates internal communications among Electronic Control Units (ECUs), sensors, and actuators through protocols such as CAN and FlexRay, establishing the vehicle's operational core [19]. The *V2X Communication* layer expands connectivity beyond the vehicle, using standards such as DSRC and C-V2X to link vehicles with each other, infrastructure, pedestrians, and external networks [20]. Lastly, the *Cloud/IoT Integration* layer links vehicles with cloud resources and IoT systems, supporting services such as OTA updates and predictive maintenance [21]. These layers' interdependence-through gateways, OBUs, and cellular interfaces-amplifies security risks, as vulnerabilities in one layer can propagate across others [22]. To understand cross-layer data flow, we first examine the specific technologies, applications, and security challenges within each telematics layer.

3.1. Intra-vehicle network

The Intra-Vehicle Network layer serves as the foundational communication infrastructure within modern vehicles, interconnecting ECUs to manage critical functions such as engine control, braking, and advanced driver-assistance systems (ADAS) [19]. This layer employs diverse protocols-such as CAN, LIN, FlexRay, and Automotive Ethernet-to facilitate real-time data exchange among ECUs, sensors, and actuators, forming the vehicle's internal nervous system [20]. Its integration with external layers, such as V2X via gateways or Cloud/IoT through diagnostic ports, amplifies its role in telematics, enabling seamless data flows for safety and performance [22]. As prior analyses have shown, the layer's legacy designs and growing connectivity create security risks. Therefore, a detailed examination of its protocols, components, applications, and vulnerabilities is required (Figs. 1, 2).

3.1.1. Protocols and components

The Intra-Vehicle Network layer relies on a range of protocols and components tailored to automotive needs, balancing cost, speed, and reliability to enable communication across diverse vehicle functions [19]. The primary protocols used are CAN, LIN, FlexRay, and Automotive Ethernet. As shown in the architectural model (Fig. 3), each is designed for distinct functions and interacts with essential components such as ECUs, gateways, and diagnostic ports.

Controller Area Network. The Controller Area Network (CAN), introduced by Bosch in 1986, is a multi-master, broadcast protocol operating at speeds up to 1 Mbps over a two-wire bus [23]. It connects critical ECUs managing engine control, braking, and transmission by sending messages that specify, for example, the vehicle's speed or throttle status, which are then processed by other ECUs based on their identifiers [20]. CAN's flexibility supports integration with gateways and OBD-2 ports, facilitating data relay to V2X or Cloud/IoT systems, though its lack of authentication poses security risks [24].

Local Interconnect Network. Local Interconnect Network (LIN) is a cost-effective, master-slave protocol running at up to 20 kbps, managing non-critical systems such as wipers and climate controls [25]. LIN interfaces with CAN via gateway ECUs, reducing wiring complexity while supporting data flows to higher-speed networks. Its minimal design, however, limits security features [20].

FlexRay. FlexRay provides high-speed (10 Mbps), fault-tolerant communication for safety-critical applications including steering and ADAS [26]. It ensures deterministic data exchange (e.g., chassis control signals) and integrates with V2X gateways, though its complexity and lack of encryption challenge security [27].

Automotive Ethernet. Automotive Ethernet offers high-bandwidth (100 Mbps to 1 Gbps) IP-based communication for infotainment, diagnostics, and ADAS [28]. It connects to V2X and Cloud/IoT via

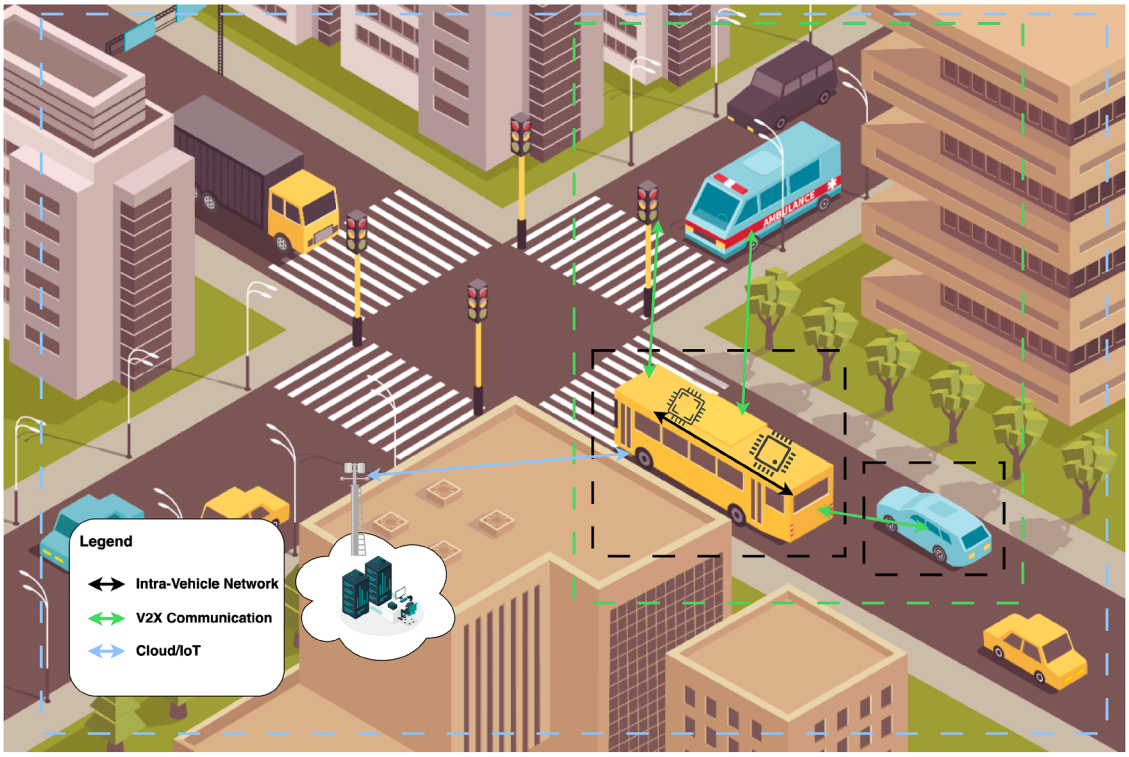


Fig. 1. A conceptual overview of the modern automotive telematics architecture, which is composed of three interconnected layers. The **Intra-Vehicle Network** governs internal vehicle functions, **V2X Communication** facilitates interaction with the external environment, and **Cloud/IoT Integration** provides connectivity to remote services. This layered model forms the foundation for the cross-layer data flow security analysis conducted in this survey.

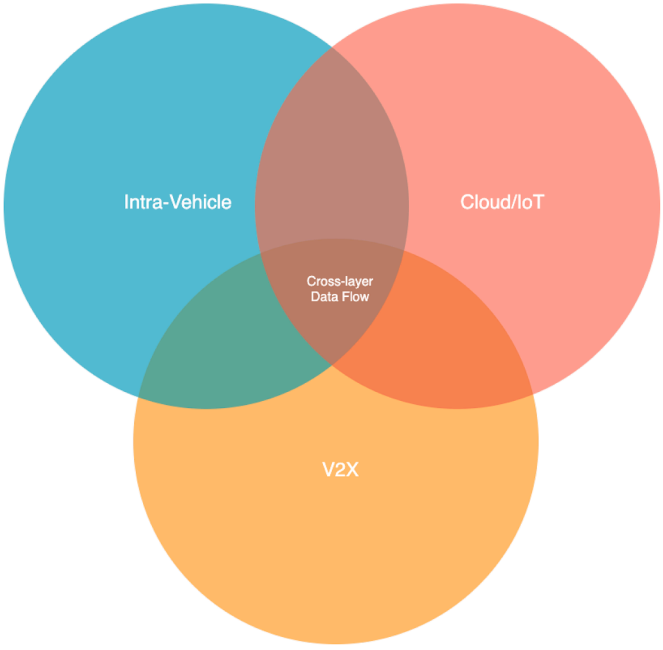


Fig. 2. Visualization of the research gap in telematics security, highlighting fragmented coverage across the **Intra-Vehicle**, **V2X**, and **Cloud/IoT** layers.

gateways, supporting multimedia and real-time data, but its openness introduces new security demands [20].

The key components that manage data flows are also potential entry points for attacks. These include ECUs (for powertrain and body control), gateways that bridge different protocols, OBD-2 ports for diagnostics, and telematics units for cellular connectivity [29].

3.1.2. Applications and use cases

Intra-Vehicle Network protocols and components enable a range of critical and auxiliary applications, each relying on seamless internal data flows and, increasingly, on integration with external telematics layers.

Engine Control. CAN-based ECUs manage engine functions by processing sensor data (e.g., oxygen levels, throttle position) to optimize fuel injection and emissions. Gateways relay this data to Cloud/IoT systems for remote diagnostics, enhancing maintenance efficiency [24].

Advanced Driving Assistance Systems. FlexRay supports ADAS by delivering the high-speed, reliable data required for lane-keeping assistance and adaptive cruise control. Integration with V2X via gateways enables real-time environmental awareness, though this connectivity risks exposing ADAS to external threats [26].

Infotainment. Automotive Ethernet drives infotainment systems, providing high-bandwidth for multimedia streaming and navigation. Cloud/IoT integration via telematics units offers real-time content updates, but IP-based vulnerabilities can compromise data integrity [28].

These applications underscore the layer's operational significance and its growing reliance on cross-layer data flows, amplifying the impact of security vulnerabilities.

3.1.3. Security challenges

The Intra-Vehicle Network's legacy protocols and expanding connectivity expose it to significant security risks, particularly at interfaces with V2X and Cloud/IoT layers. Key vulnerabilities include spoofing, eavesdropping, and cross-layer attacks, threatening data integrity and vehicle safety [30].

CAN's broadcast nature and lack of encryption allow attackers to inject spoofed messages via OBD-2 ports or Bluetooth, falsifying commands (e.g., brake signals) that could mislead V2X safety systems [31].

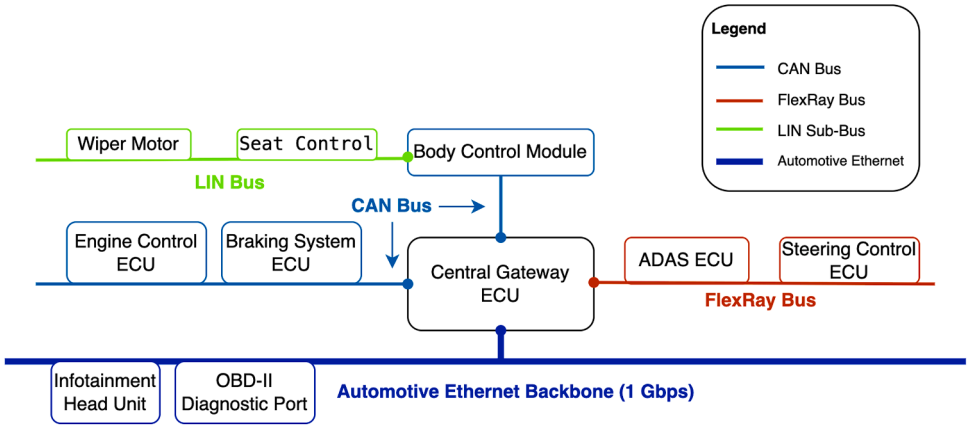


Fig. 3. A model of a modern domain-based intra-vehicle network architecture. A high-speed **Automotive Ethernet** backbone connects to a **Central Gateway ECU**, routing data between multiple domain-specific buses.

LIN's simplicity enables injection attacks through CAN gateways, potentially disrupting non-critical functions including climate control, which could distract drivers or indirectly impair operations [25]. FlexRay, despite error detection, is susceptible to eavesdropping, risking ADAS data corruption that could affect V2X message integrity [26]. Automotive Ethernet's IP-based design heightens risks of network-based attacks (e.g., replay), exposing infotainment or diagnostic data to Cloud/IoT breaches [28].

Gateways and telematics units, as bridges to external layers, are prime targets-exploits via cellular or Bluetooth links can compromise ECUs, as demonstrated in the 2015 Jeep hack, where attackers accessed the CAN bus remotely [32]. These threats highlight the need for robust, cross-layer security measures to protect intra-vehicle data flows.

3.2. V2X communication

The V2X communication layer connects vehicles with external entities (e.g., other vehicles, infrastructure, pedestrians, networks) to improve safety, traffic efficiency, and to enable advanced services such as autonomous driving [20]. Based on the DSRC and C-V2X standards, the V2X layer connects with intra-vehicle networks through On-Board Units (OBUs) and interfaces with Cloud/IoT platforms via cellular networks, creating a central hub within telematics architectures [33]. This layer's real-time data flows support applications including collision avoidance, platooning, and smart city integration, yet its external orientation amplifies security challenges at interfaces with other layers [34]. The interdependence with Intra-Vehicle systems (e.g., via gateways processing V2V data) and Cloud/IoT platforms (e.g., via V2N for navigation) creates a complex ecosystem where vulnerabilities can cascade, as seen in real-world incidents such as network jamming [27]. This subsection explores V2X's standards, applications, and security challenges, providing a foundation for cross-layer data flow security analysis.

3.2.1. Communication standards

V2X communication relies on two primary standards-Dedicated Short-Range Communication (DSRC) and Cellular V2X (C-V2X)-each facilitating data exchange with distinct technical foundations [20]. These standards bridge Intra-Vehicle networks via OBUs and Cloud/IoT systems through cellular or roadside infrastructure [27].

IEEE 802.11p-Based. DSRC, built on IEEE 802.11p, operates in the 5.9 GHz band, offering short-range (up to 1 km), low-latency communication for V2V and V2I applications [35]. Standardized as C-ITS in the EU, ITS Connect in Japan, and part of the IEEE 1609 WAVE suite in the U.S., DSRC uses a Wi-Fi-derived protocol to transmit specific message sets, for instance Basic Safety Messages, via OBUs and Roadside Units (RSUs) [20]. Released in 2010, it aimed to enhance safety by linking Intra-Vehicle systems for real-time responses. However, its limited deployment-hampered by scalability and reliability issues-led the U.S. FCC to reallocate much of its spectrum in 2020, favoring C-V2X's broader adoption [36].

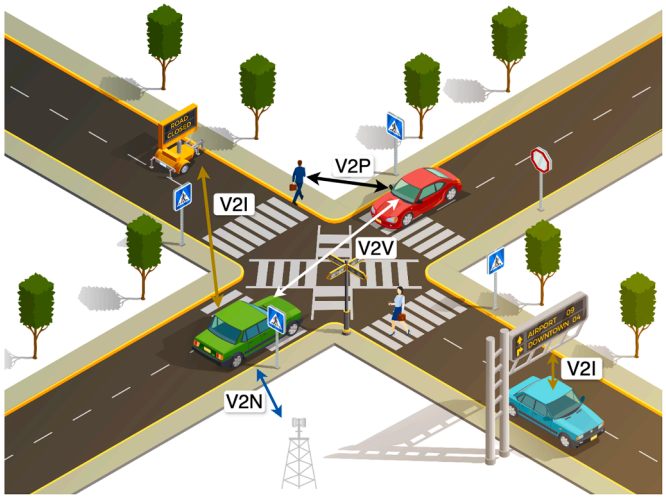


Fig. 4. Illustration of the **V2X** ecosystem at a smart intersection, highlighting communication between **vehicles**, **infrastructure**, **pedestrians**, and **networks**.

C-V2X. C-V2X, defined by the 3GPP, evolved from LTE-V2X (Release 14, 2016) to 5G NR-based standards (Release 16, 2020), expanding V2X capabilities [27]. It supports dual modes: direct short-range communication via the PC5 sidelink interface (e.g., V2V, V2I) and long-range network communication via the Uu interface (e.g., V2N, V2P), covering all V2X types [34]. This adaptability links pedestrian devices and cloud servers, improving data exchange with Intra-Vehicle networks and Cloud/IoT platforms for applications such as remote diagnostics [20].

3.2.2. Applications and use cases

V2X communication enables diverse applications by facilitating data exchanges between vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and networks (V2N), as depicted in Fig. 4. These exchanges improve safety, efficiency, and user experience while relying on seamless integration with Intra-Vehicle and Cloud/IoT layers.

Collision Avoidance. V2V supports collision avoidance by enabling vehicles to exchange real-time data (e.g., speed, position) via Basic Safety

Messages. OBUs transmit this information to Intra-Vehicle ECUs, enabling immediate braking or steering adjustments to mitigate risks during sudden lane changes or similar events [37].

Traffic Optimization. V2I facilitates traffic optimization by connecting vehicles to RSUs at traffic signals or intersections. Real-time updates (e.g., signal timing, congestion alerts) integrate with Intra-Vehicle navigation systems, improving flow and reducing delays, often enhanced by Cloud/IoT traffic analytics for city-wide coordination [38].

Pedestrian Safety. V2P enhances safety by linking vehicles to pedestrian smart devices via C-V2X's PC5 interface, alerting drivers to nearby vulnerable road users (e.g., at crosswalks). Cloud/IoT systems aggregate pedestrian data, aiding broader safety efforts such as urban mobility planning [39].

Vehicle Platooning. V2V enables platooning, where vehicles travel closely in convoy, sharing speed and braking data to optimize fuel efficiency and road capacity. This relies on Intra-Vehicle control systems for synchronized responses and Cloud/IoT for route planning [34].

Remote Services. V2N links vehicles with cellular networks, providing cloud-based services such as navigation, OTA updates, and entertainment. This links Intra-Vehicle systems to Cloud/IoT platforms, enabling real-time route adjustments or firmware enhancements, critical for modern fleets [33].

3.2.3. Security challenges

V2X communication's dependence on real-time, interconnected data flows broadens its attack surface, exposing it to privacy and availability threats at interfaces with Intra-Vehicle networks and Cloud/IoT systems [20]. These vulnerabilities can disrupt safety-critical operations and cascade across layers [33].

Privacy risks stem from V2X's extensive data exchanges. V2V and V2I messages (e.g., Cooperative Awareness Messages) broadcast vehicle positions and identifiers, enabling location tracking via compromised RSUs or network intercepts [40]. V2P's cellular links risk exposing pedestrian data (e.g., movement patterns), while V2N's cloud connectivity heightens leakage potential for driving habits, with breaches potentially reaching Intra-Vehicle systems via OBUs [39]. Such privacy violations can propagate to Cloud/IoT platforms, compromising user trust [41].

Availability threats undermine V2X's integrity. Denial-of-service (DoS) attacks can flood V2V channels with fake messages, delaying collision avoidance responses linked to Intra-Vehicle ECUs (e.g., falsified braking signals) [34]. Jamming disrupts V2I traffic updates, impairing navigation or platooning coordination, while V2N faces network-based DoS, severing cloud services that include OTA updates or real-time maps [38]. In dense urban environments, scalability exacerbates these risks, with interference or resource exhaustion disrupting Cloud/IoT reliability and potentially halting smart city functions [42]. These challenges necessitate comprehensive, cross-layer security solutions, explored in subsequent analyses.

3.3. Cloud/IoT integration

The Cloud/IoT Integration layer interfaces vehicles with cloud resources and IoT systems, supporting advanced services such as OTA updates, remote diagnostics, and smart city applications [43]. Leveraging technologies such as cloud computing, edge processing, and 5G networks, this layer aggregates data from Intra-Vehicle networks via diagnostic ports and V2X communication through V2N links, forming a critical hub in automotive telematics [33]. Its capabilities facilitate real-time applications such as autonomous driving and traffic management, improving vehicle functionality and user experience. However, its extensive reliance on external connectivity and data processing amplifies security risks, as vulnerabilities can propagate to V2X channels (e.g., via V2N breaches) or Intra-Vehicle systems (e.g., through tampered OTA updates) [21]. This subsection explores the layer's technologies, applications, and security challenges, culminating in a synthesis that transitions to cross-layer data flow security analysis.

3.3.1. Key technologies and architectures

The Cloud/IoT Integration layer employs advanced technologies and architectures to facilitate connectivity, data processing, and service delivery, addressing challenges including latency and scalability in vehicular environments.

Cloud Computing. Cloud computing forms the backbone of the Cloud/IoT layer, providing centralized, scalable resources for storage and computation. In automotive telematics, cloud platforms handle extensive data streams from connected vehicles, supporting services such as remote diagnostics and traffic pattern analysis. For instance, cloud servers process telemetry data to predict component failures, enhancing reliability and reducing costs [21]. However, the distance to remote servers introduces latency, presenting challenges for delay-sensitive tasks such as real-time hazard detection [43]. Cloud scalability also supports OTA updates, though vulnerabilities in such systems require robust security measures [44].

Edge Computing. Edge computing mitigates latency by bringing processing closer to the vehicle or roadside infrastructure. Paradigms such as Multi-Access Edge Computing (MEC) and Vehicular Edge Computing (VEC) deploy resources at RSUs or within vehicles, facilitating rapid decision-making. MEC processes sensor data at the edge for immediate collision avoidance, crucial for safety-critical applications [45]. VEC leverages nearby RSUs to offload tasks, reducing reliance on distant clouds and enhancing responsiveness [21,43]. These edge approaches complement cloud computing by balancing real-time needs with large-scale analytics.

IoT Devices. Fundamental to the Cloud/IoT layer are various IoT devices, which include the sensors and actuators in vehicles and infrastructure. They collect real-time data-e.g., speed, location, and environmental conditions-feeding into cloud and edge systems. Asset tracking is enabled by technologies such as Radio-Frequency Identification (RFID), while Ultra-Wideband (UWB) supports precise positioning within vehicular networks [43]. For example, RFID streamlines toll collection, and UWB enhances intra-vehicle sensor communication, improving operational efficiency and user convenience.

Communication Technologies. Robust communication technologies ensure reliable data exchange. High-bandwidth 5G networks provide low-latency, high-throughput connectivity for live traffic updates and remote control [46]. Emerging 6G promises further enhancements, supporting autonomous driving and V2X communication [43]. For less time-sensitive tasks, Narrowband-IoT (NB-IoT) and Long-Range (LoRa) offer energy-efficient, wide-area coverage, ideal for vehicle health monitoring and fleet management [43]. Vehicular Fog Computing (VFC) integrates fog nodes-e.g., parked vehicles-to enhance local processing and reduce congestion [21].

Data Management. The exponential growth of vehicular data requires sophisticated management. Big data analytics, powered by AI and ML, extract insights from IoT device data. Cloud-based federated learning models analyze driving patterns securely for predictive maintenance [33], while edge processing filters data to optimize bandwidth [43]. Anomaly detection, supported by analytics, identifies mechanical issues early, enhancing safety and efficiency [21,47].

3.3.2. Applications and use cases

The Cloud/IoT Integration layer enables a range of automotive applications by leveraging cloud computing, edge processing, IoT devices, and advanced communication technologies. These use cases enhance vehicle functionality, safety, and urban integration, relying on seamless data flows across telematics layers.

OTA Updates. OTA updates deliver remote software enhancements to vehicle systems, such as ECUs and infotainment, eliminating physical recalls. Cloud platforms manage update distribution, while edge nodes verify integrity, improving efficiency and safety [21]. Secure OTA designs reduce overhead by 52%, supporting firmware upgrades critical for modern vehicles [48].

Remote Diagnostics and Monitoring. Real-time diagnostics and predictive maintenance rely on IoT sensors to track vehicle health, with cloud analytics forecasting potential issues, such as engine wear. This enhances reliability by analyzing telemetry data remotely [49]. IoT-enabled monitoring tracks performance metrics, offering proactive maintenance solutions for fleet management [43].

Infotainment Services. Infotainment services provide streaming media, real-time navigation, and personalized content through cloud resources. High-bandwidth 5G networks ensure low-latency delivery, while edge computing supports seamless playback [43]. These services enhance driver experience by integrating multimedia and navigation data from the cloud.

Autonomous Driving Support. Autonomous driving relies on cloud-supplied high-definition maps and traffic data, processed with federated learning for secure decision-making [33]. Edge computing handles delay-sensitive tasks involved in obstacle detection, complementing cloud analytics for route planning [21]. This synergy enables safer, efficient self-driving capabilities.

Smart City Integration. Smart city integration connects vehicles to urban infrastructure via IoV, optimizing traffic flow and reducing emissions. Cloud/IoT systems facilitate vehicle-to-infrastructure communication, supported by federated learning for efficient traffic management [50]. Real-time data exchange enhances urban mobility and sustainability [43].

3.3.3. Security challenges

The Cloud/IoT Integration layer's extensive connectivity and data processing amplify its exposure to security threats, impacting privacy, integrity, and availability across telematics interfaces with V2X and Intra-Vehicle layers [43]. These challenges arise from the layer's reliance on cloud resources, edge nodes, and IoT devices, necessitating robust safeguards.

Data privacy poses a significant risk, as vast amounts of sensitive information (including a user's location, driving habits, and personal preferences) are collected by IoT sensors and stored in the cloud. Unauthorized access via cellular networks or cloud breaches can expose this data, affecting user trust and safety [39]. For instance, V2N communications transmitting diagnostics or infotainment data heighten privacy concerns, with potential leaks propagating to external systems [43]. Federated learning approaches aim to mitigate this, but vulnerabilities persist [33].

Authentication and authorization vulnerabilities threaten remote access to vehicle functions. Weak mechanisms in OTA update systems or cloud-managed diagnostics allow attackers to impersonate legitimate entities, potentially delivering malicious software [51]. Such breaches could compromise ECUs via V2X gateways, disrupting Intra-Vehicle operations [21]. The integrity of data is equally critical. Tampered OTA updates risk altering vehicle behavior, endangering safety [44]. This threat to data integrity also extends to operational data. For instance, cloud analytics datasets are vulnerable to data poisoning. In these attacks, adversaries systematically inject malicious data to corrupt the output of the prediction model [52].

Availability challenges stem from DoS attacks targeting cloud services or communication links, disrupting real-time applications, for example, autonomous driving and smart city integration. DoS can overwhelm 5G networks or edge nodes, delaying critical traffic updates or HD map delivery [42]. In dense urban settings, scalability exacerbates these risks, as resource exhaustion impacts Cloud/IoT reliability [21].

Cross-layer vulnerabilities compound these issues, as weaknesses in Cloud/IoT can cascade to other layers. Exploits via V2N could infiltrate Intra-Vehicle networks through diagnostic ports, while edge-cloud interactions risk amplifying attacks across V2X channels [53]. These interconnected threats underscore the need for comprehensive security solutions to protect Cloud/IoT data flows, as visually summarized in Fig. 5.

3.4. Conclusion and transition to data flow security analysis

The telematics layers-Intra-Vehicle Network, V2X Communication, and Cloud/IoT Integration-form a cohesive backbone for automotive systems, enabling seamless data flows for safety, efficiency, and connectivity [20]. Intra-vehicle protocols, notably CAN, ensure internal coordination but also face significant spoofing risks [31]. In the external domain, V2X standards such as DSRC and C-V2X extend connectivity but introduce new privacy and jamming threats [34]. The integration of Cloud/IoT improves functionality through OTA and autonomy; yet, its dependence on these technologies leads to privacy and integrity issues [43]. Risks are increased by their interconnection through gateways, V2N, and diagnostic ports, since breaches spread throughout layers [21]. These challenges, from Intra-Vehicle spoofing to Cloud/IoT DoS attacks [42], highlight the importance of robust data flow security. The following analysis examines approaches including federated learning [33] and proactive protocols [53] for protecting telematics systems.

4. Data flow security

Having detailed the distinct functions, technologies, and inherent security challenges of the Intra-Vehicle Network, V2X Communication, and Cloud/IoT Integration layers in Section 3, we now shift focus to the critical aspect of securing the data flow within and across these interconnected domains. The effectiveness of the telematics ecosystem depends on maintaining the confidentiality, integrity, and availability of data across internal buses, wireless links, and cloud interfaces. Protecting this flow requires addressing diverse threats ranging from internal message spoofing to external eavesdropping and ensuring secure transitions between different protocols and security domains. This section systematically surveys and analyzes recent security solutions proposed for these challenges, categorized by the specific layer or interface they target: Intra-Vehicle Layer security (Section 4.1), V2X Communication Layer security (Section 4.2), and Interface-Specific security (Section 4.3). Our analysis emphasizes crucial security properties, including intrusion detection, privacy, availability, and authentication, comparing methods based on threat models, efficiency, and scalability to highlight progress and identify remaining gaps.

4.1. Intra-vehicle layer security solutions

The Intra-Vehicle Layer, detailed in Section 3.1, forms the vehicle's internal communication backbone. Protocols such as CAN, LIN, and FlexRay are essential for coordinating vehicle components, but their legacy designs create significant security vulnerabilities. Commonly used protocols, particularly CAN, lack built-in authentication and encryption. This vulnerability exposes them to attacks such as message spoofing and replay, potentially compromising safety-critical functions such as braking and steering [2,19]. Compounding these vulnerabilities

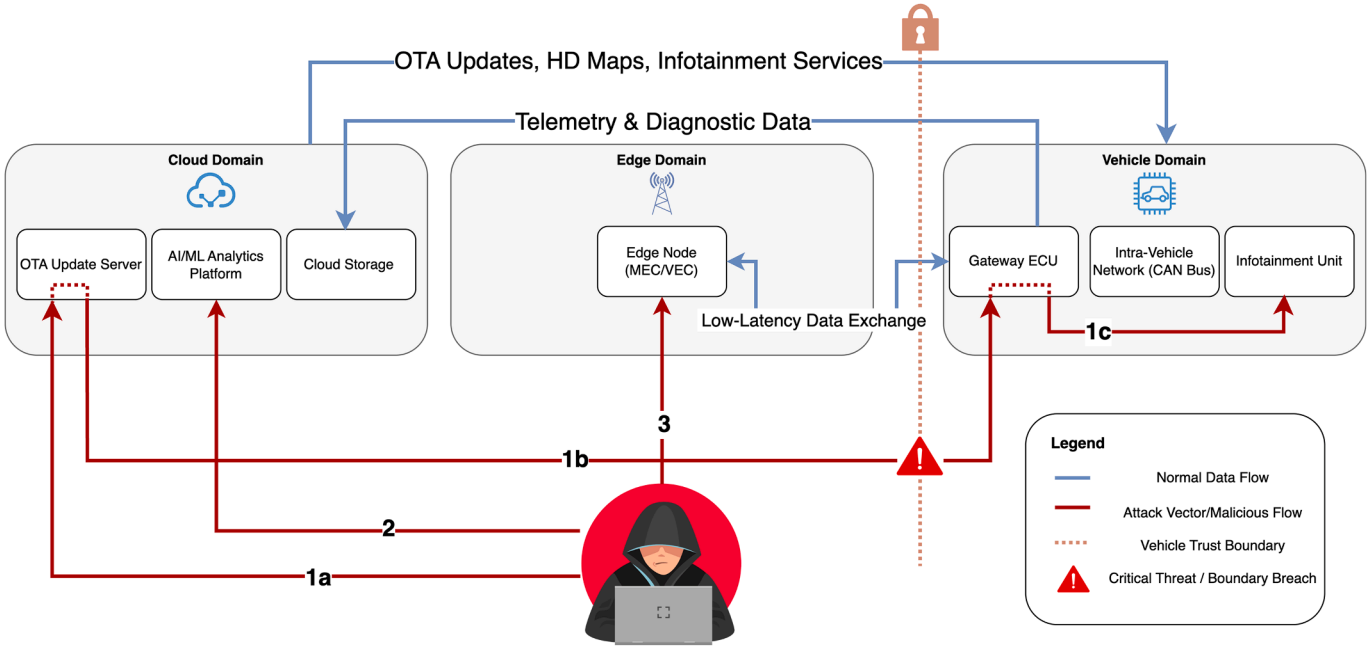


Fig. 5. A threat model illustrating cross-layer vulnerabilities in the telematics ecosystem. Normal data flows (blue) and malicious attack vectors (red) are shown across the Cloud, Edge, and Vehicle domains. The model highlights a cascading attack chain: **(1a)** an adversary compromises the cloud-based OTA Server; **(1b)** a tampered update is delivered across the Vehicle Trust Boundary, indicated by the warning icon; and **(1c)** the threat propagates into the safety-critical Intra-Vehicle Network. The model also depicts parallel threats, including **(2)** a data poisoning attack on the AI/ML Platform and **(3)** a DoS attack targeting the Edge Node. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

are the stringent operational constraints: ECUs typically offer limited computational power and memory, while security mechanisms must introduce minimal latency to avoid disrupting real-time control loops [26,32]. Research addressing these challenges primarily divides into two categories, discussed in detail: first, IDS solutions monitoring network traffic for anomalies and malicious behavior (Section 4.1.1), and second, proactive methods ensuring Secure Communication and Data Integrity through measures such as authentication and encryption (Section 4.1.4).

Take the CAN bus, for example, a protocol ubiquitous in vehicles since the 1980s. Its lack of built-in authentication means any device on the network can send commands, such as accelerating or braking, without verifying its identity, enabling spoofing attacks where malicious messages mimic legitimate ones. Similarly, the absence of encryption leaves data transmissions exposed to eavesdropping, while the bus's broadcast nature makes it prone to replay attacks (re-sending captured messages) and DoS attacks that flood the network, delaying critical commands. An infamous real-world case occurred in 2015 with the remote hack of a Jeep Cherokee. Researchers manipulated the vehicle's CAN bus to disable its brakes and steering, an exploit that ultimately led to the recall of 1.4 million vehicles. Such incidents underscore the dire consequences of unsecured intra-vehicle communication, threatening not just vehicle performance but the safety of passengers and other road users.

Securing this layer is challenging due to the resource constraints of ECUs and the real-time performance demands of automotive systems. ECUs, the computational workhorses of the Intra-Vehicle Layer, are typically resource-constrained with limited processing power, memory, and energy. These conditions are ill-suited for traditional security tools that require heavy encryption. Moreover, automotive systems demand security measures operating with minimal latency to avoid interference with critical, time-sensitive functions such as collision avoidance. Adding to the complexity is the heterogeneity of protocols: legacy CAN systems coexist with newer FlexRay and automotive Ethernet, each with distinct strengths and weaknesses, making a one-size-fits-all solution impractical. These challenges highlight the urgent need for innovative, tailored approaches to safeguard data integrity, confidentiality, and availability within the vehicle.

This section explores recent advancements in securing the Intra-Vehicle Layer, organized around two key themes: IDS and Secure Communication and Data Integrity. IDS solutions, often leveraging ML or statistical models, monitor network traffic to detect anomalies, such as unexpected message patterns, offering a lightweight way to flag attacks in real time. In contrast, Secure Communication and Data Integrity approaches use proactive cryptographic techniques, for instance message authentication codes (MACs) or lightweight encryption, to prevent tampering and unauthorized access. Both strategies aim to address the layer's vulnerabilities while respecting its operational constraints. In the following analysis, we review these solutions, comparing their threat models (e.g., what attacks they counter), efficiency (e.g., resource usage), and scalability (e.g., applicability across vehicle types). Our goal is to assess their effectiveness and suitability for automotive applications, identify gaps in current research (such as handling emerging threats or integrating with V2X systems), and propose directions for future work to ensure the Intra-Vehicle Layer remains a robust foundation for next-generation vehicles.

4.1.1. Intrusion detection systems

IDS play a critical role in safeguarding intra-vehicle communication by continuously monitoring network traffic to detect malicious activities or anomalies indicative of cyber threats. Modern vehicles increasingly rely on electronic components interconnected through protocols such as CAN, Automotive Ethernet, and FlexRay. Because these protocols often lack built-in authentication, encryption, and integrity checks, they are vulnerable to cyberattacks that can compromise vehicle safety and reliability.

Recent literature presents a wide range of IDS approaches designed specifically for intra-vehicle network security. Existing IDS research can be categorized into three main approaches: ML-based, statistics-based, and hybrid models, all of which depend on high-quality benchmark datasets for evaluation.

- **ML-based IDS**, leveraging sophisticated algorithms and models to detect complex attack patterns within intra-vehicle networks.
- **Statistics-based IDS**, utilizing computationally efficient statistical methods and are often lightweight algorithms suitable for embedded environments with stringent resource constraints.
- **Benchmark Datasets**, offering realistic, well-labeled data essential for rigorous validation, training, and comparative evaluation of IDS solutions.

After reviewing these categorized solutions, the section concludes with a comparative analysis and synthesis, highlighting strengths, limitations, practical implications, and opportunities for future research.

Solution Summaries.

ML-based IDS. ML-based intrusion detection systems represent a significant category of IDS solutions, leveraging sophisticated algorithms to accurately identify malicious activities within intra-vehicle networks, particularly targeting the vulnerable CAN and automotive Ethernet communication protocols.

Several studies apply deep learning to secure the CAN bus against DoS and spoofing attacks. Song et al. [19] use a DCNN to analyze traffic patterns, achieving high accuracy but facing challenges in resource-limited environments. Chougule et al. [31] enhance detection with a two-step LSTM-CNN model, reaching 99.5% accuracy at the cost of computational demands. Khandelwal et al. [32] address efficiency by deploying a quantized DCNN on FPGA hardware, maintaining accuracy while significantly reducing energy use, though requiring specialized hardware. Mansourian et al. [54] propose a prediction-based IDS framework utilizing LSTM and ConvLSTM networks to detect anomalies and attacks on the CAN bus by leveraging temporal and spatiotemporal correlations, achieving nearly 100% detection accuracy on the Car Hacking Dataset via a Gaussian Naïve Bayes classifier on prediction errors. In contrast to deep learning, Alfardus and Rawat [55] introduce a modular IDS that employs traditional ML algorithms, achieving near 100% accuracy against impersonation and fuzzy attacks, though noting varied execution times depending on the specific algorithm used.

Zenden et al. [30] highlight the vulnerability of ML-based IDS to adversarial attacks where crafted inputs can cause the model to misclassify threats, and they advocate for adversarial training to enhance robustness. Beyond inputs designed for misclassification, these data-driven models are also susceptible to data poisoning attacks, where an adversary corrupts the underlying dataset to compromise the system's performance, a threat formally modeled by Wang et al. [52]. To counter such vulnerabilities, He et al. [56] propose a defense-aware robust reinforcement learning (DARRL) framework that trains a driving policy to be inherently resilient to worst-case sensor data attacks through an adversarial attacker-defender paradigm.

Song et al. [57] and Zhang et al. [58] address the scarcity of labeled attack data, employing self-supervised learning to detect unknown attacks and federated learning for privacy-preserving rapid detection, respectively.

Unlike CAN bus-focused approaches, Jeong et al. [28] develop a CNN-based IDS for automotive Ethernet, achieving high accuracy and real-time detection of replay attacks on AVTP streams.

These studies collectively highlight the diverse potential and inherent challenges associated with implementing ML-based IDS in vehicular networks, underscoring considerations regarding computational overhead, real-time applicability, and adversarial resilience.

Statistics-based IDS. For resource-constrained automotive contexts, statistics-based IDS can safeguard IVNs by striking a balance between low processing cost and detection accuracy. These techniques identify significant deviations as intrusions and build a statistical model of typical network traffic based on time, message frequency, or information entropy. While contemporary research is developing hybrid models, foundational strategies rely on statistical measurements. These sophisticated systems enhance detection performance and robustness by combining ML and statistical techniques.

Liu et al. [23] propose a lightweight IDS using information entropy and KL divergence for real-time anomaly detection on the CAN bus, achieving over 98% accuracy against DoS attacks.

Wei et al. [26] present a real-time IDS using EDF scheduling and queue forwarding efficiency to improve data throughput and reduce false detections in CAN and FlexRay gateways.

Hao et al. [59] present a hybrid statistical-ML model using a SARIMA model to generate dynamic detection thresholds, which are supplemented by an LSTM model to ensure high detection accuracy and prevent model corruption during cyberattacks.

Goina et al. [60] introduce Statistical Aggregated Anomaly Detection (SAAD), a methodology that aggregates the results from a histogram-based statistical method and a Fully Connected Network (FCN) to improve performance, boosting detection accuracy from approximately 72% for the standalone models to 88.3% for the combined approach.

Statistics-based IDS research has progressed from lightweight standalone methods to strong hybrid systems. Statistical analysis for embedded environments is effective with information theory-based approaches and traffic parameter monitoring, although static thresholds or environmental volatility can limit them. Statistical-ML hybrid models, including SARIMA-LSTM and SAAD, are increasingly adopted for data correction and outcome aggregation. By combining statistics and ML, these integrated systems achieve a level of precision and robustness that neither approach can supply on its own.

Benchmark Datasets. Developing, training, and evaluating automotive IDS effectively requires high-quality benchmark datasets that simulate realistic network environments and attack scenarios. Realistic and accurately labeled datasets enable comprehensive performance assessment, promoting the advancement of reliable IDS solutions by simulating authentic IVN environments and attack scenarios.

Van der Heijden et al. [61] introduced the Vehicular Reference Misbehavior (VeReMi) dataset, the first public, extensible dataset for evaluating misbehavior detection in VANETs. It consists of simulated message logs from the LuST scenario with varying traffic densities and includes a labeled ground truth for different types of simple position falsification attacks.

Kamel et al. [62] present the VeReMi Extension, a large-scale simulated dataset for misbehavior detection in VANETs, enhancing the original VeReMi dataset with a realistic sensor error model and a diverse set of new attacks including data replay, DoS, and Sybil attacks, all generated within the Luxembourg SUMO Traffic (LuST) scenario.

Netto et al. [24] introduce CICIoV2024, a benchmark dataset for CAN bus intrusion detection, featuring realistic DoS and spoofing attacks from a 2019 Ford vehicle.

Lampe et al. [29] introduce a curated CAN dataset from four vehicles, covering nine attack scenarios including gear spoofing and DoS, available in various formats for IDS evaluation.

Together, these datasets significantly enhance the ability of researchers and practitioners to develop and rigorously evaluate automotive IDS, thus directly contributing to improved cybersecurity resilience within vehicular telematics systems (Table 2).

4.1.2. Comparative analysis

The comparative analysis reveals several common themes and trade-offs across the surveyed IDS, with key attributes of prominent studies summarized in Table 3.

Threat Model Focus: A predominant focus across many IDS solutions is the mitigation of attacks exploiting the vulnerabilities of the widely deployed CAN bus, particularly DoS and message spoofing/injection attacks [19,23,31,32,55]. This reflects the legacy nature and inherent lack of security in CAN. At the same time, research is increasingly focusing on threats targeting modern protocols such as Automotive Ethernet, addressing issues including replay attacks on AVTP streams [28]. Another emerging challenge involves securing ML-based IDS from ad-

Table 2
Comparative analysis of benchmark datasets for automotive intrusion and misbehavior detection.

Dataset	Domain	Generation Method	Attack Types	Features	Contributions
VeReMi (2018) [61]	VANET (V2X)	Simulation (LuST scenario)	Position falsification (e.g., constant, random offset)	Extensible, labeled, GPS logs	First public benchmark for VANET misbehavior detection
VeReMi Extension (2020) [62]	VANET (V2X)	Simulation (with error models)	DoS, replay, Sybil, malfunction emulation	Sensor error model, pseudonym changes, attack-onset labels	Realism improvements over original VeReMi
can-train-and-test (2024) [29]	In-Vehicle (CAN)	Real vehicles (on-road, 4 models)	DoS, spoofing, fuzzing, gear/speed spoofing	Replayable logs, labeled/unlabeled CSVs, train/test splits	Generalizability to unseen vehicles and attacks
CICIoV2024 (2024) [24]	In-Vehicle (CAN)	Real-world testbed (2019 Ford, full ECUs)	DoS, spoofing (RPM, gas, speed, steering)	Binary, decimal, hex formats	High-fidelity CAN dataset with complete in-vehicle structure

Table 3
Comparative analysis of ids methods for IVNs.

Study	Approach & Proactivity	Threat Model	Key Results/Trade-offs
Reactive Detection Approaches			
Song et al. [19]	DCNN	DoS, spoofing	High accuracy, low latency; ECU constraints noted.
Chougule et al. [31]	LSTM-CNN	Spoofing, fuzzing, DoS	99.5% accuracy; moderate overhead.
Khandelwal et al. [32]	FPGA DCNN	Injection, spoofing	99% accuracy; energy-efficient via hardware.
Mansourian et al. [54]	LSTM, ConvLSTM	Anomalies, DoS, Fuzzy, Spoofing	Almost 100% F-score/accuracy on Car Hacking Dataset ; addresses temporal/spatiotemporal correlations.
Zhang et al. [58]	Federated GNN	Message injection	Rapid (~3ms), scalable, privacy-preserving.
Jeong et al. [28]	CNN AVTP	Replay attacks	High accuracy (F1 = 0.97) for Ethernet streams.
Alfardus & Rawat [55]	ML-based	Impersonation, fuzzy	Near-perfect accuracy; variable speeds.
Proactive and System-Level Approaches			
Zenden et al. [30]	Adversarial Training	Adversarial attacks	Improved robustness against evasion.
Song et al. [57]	Self-supervised Learning	Unknown attacks	Efficient detection of unknown anomalies.
He et al. [56]	Robust RL	Sensor perturbations	Policy resilient under sensor attacks.

versarial manipulation [30]. This now also includes creating controllers resilient to direct attacks on sensor data, such as the *observational perturbations* investigated by He et al. [56], which represent a threat to the perceptual data flow itself.

Detection Approaches and Proactivity: While most IDS function reactively, detecting anomalies or known attack patterns in real-time [19,23,31], there is a discernible trend towards incorporating proactive elements. Techniques such as self-supervised learning aim to identify unknown or zero-day attacks by detecting deviations from normal behavior, even when attack data is scarce [57]. Similarly, adversarial training is explored as a proactive measure to harden ML models against evasion attempts before deployment [30]. An even more advanced proactive strategy is presented by He et al. [56], who use a defense-aware reinforcement learning framework to train a driving policy that is robust-by-design, moving beyond hardening a model to creating one that is inherently resilient through a game-theoretic attacker-defender paradigm. Hybrid approaches, such as the two-step LSTM-CNN model in HybridSecNet [31], attempt to balance broad anomaly detection with specific attack classification.

Efficiency and Scalability Challenges: Given the real-time requirements and resource-constrained nature of automotive ECUs, efficiency is a critical and commonly addressed challenge. Lightweight statistical methods leveraging information theory demonstrate high accuracy with minimal overhead [23]. Complex Deep Learning models achieve substantial efficiency gains through methods including quantization and specialized hardware deployments, such as FPGAs, significantly lowering energy use and latency compared to GPU-based implementations [32]. In contrast, proactive training methods such as the defense-aware reinforcement learning proposed by He et al. [56] can introduce significant computational overhead during the training phase due to the need to simulate an adversarial attacker, though the resulting policy is efficient at deployment. Scalability, especially regarding data management and privacy across varied vehicle fleets and conditions, increasingly relies on distributed methods such as federated learning. This approach facilitates collaborative model training without centralizing sensitive CAN data [58].

Validation and Reported Accuracy: The validation strategies for the surveyed solutions are becoming increasingly sophisticated, moving beyond private data captures toward public benchmarks that ensure reproducible results. The methods are evaluated against a diverse range of these benchmarks, which vary in scope and fidelity. These include in-vehicle CAN datasets captured from real-world vehicles and testbeds (e.g., can-train-and-test [29], CICIoV2024 [24]) and large-scale simulated VANET datasets designed for misbehavior detection (e.g., VeReMi [61] and its extension [62]). The shift toward specialized, publicly available datasets, combined with hardware testbeds [32] and datasets designed for specific threats such as adversarial attacks [30], is essential for thoroughly evaluating IDS performance and applicability. High detection accuracy is frequently reported across various approaches, with ML-based and hybrid systems often exceeding 98–99% [23,31,32] or showing significant performance gains through aggregation [60].

Key Trade-offs: Synthesizing these findings highlights a fundamental trade-off between the potential high accuracy of sophisticated ML models and the stringent efficiency demands of embedded automotive systems. Strategies including hardware acceleration [32], lightweight statistical algorithms [23], hybrid architectures [31], and distributed learning paradigms [58] are widely used to maintain optimal performance. Furthermore, research into robust-by-design AI introduces a critical trade-off between optimal performance and guaranteed safety under attack. The framework by He et al. [56], for example, explicitly constrains the agent's policy to ensure safety, which may result in more conservative, but trustworthy, driving behavior. The reliance on data

quantity and quality for training robust ML models also remains a common challenge, addressed partly by self-supervised [57] and federated [58] techniques.

4.1.3. Synthesis

Synthesizing the insights from the reviewed studies, it is clear that effective IDS in vehicular networks hinges on balancing computational efficiency and detection accuracy. A hybrid approach could be optimal, merging lightweight statistical methods for real-time baseline monitoring with ML techniques to tackle sophisticated or unknown attacks. Furthermore, the most advanced research suggests a future direction beyond just detecting intrusions, focusing instead on developing inherently trustworthy AI controllers that are robust and secure by design against attacks on their perceptual data. Moreover, improving dataset quality and diversity through collaborative and interdisciplinary efforts remains critical for advancing IDS performance. As these systems develop, their ability to identify anomalies at key transition points-such as gateway interfaces linking internal networks to external systems-will play a vital role in securing the broader telematics architecture, ensuring threats are caught before they propagate across layers.

4.1.4. Secure communication and data integrity

Within the intra-vehicle network layer, secure communication and data integrity are paramount to ensure the reliability, functionality, and safety of modern automotive systems. The increasing reliance on ECUs and CAN buses for safety-critical functions makes them vulnerable to attacks that include message spoofing and tampering. Consequently, they require strong security measures. Recent approaches to intra-vehicle security use authentication and encryption to reinforce message integrity and ECU trustworthiness. These methods are designed explicitly to mitigate vulnerabilities in conventional protocols that lack built-in security. The following section summarizes notable methods employing blockchain technologies and cryptographic solutions aimed at securing communication and ensuring the authenticity and integrity of in-vehicle data.

Solution Summaries.

Blockchain-based Solutions. Blockchain technologies provide decentralized frameworks capable of securely recording and verifying ECU states and interactions. Oham et al. [22] propose B-FERL, a blockchain-based framework specifically designed to ensure ECU integrity within smart vehicles. Utilizing a two-tiered, permissioned blockchain architecture, B-FERL securely records critical ECU state transitions, allowing trusted entities to verify ECU integrity in real time via challenge-response interactions. This decentralized approach enhances resistance to insider threats and central-point failures; however, latency challenges emerge as a potential issue when scaling the system across large vehicle fleets, necessitating optimization for practical deployment.

Lightweight Authentication Methods. To meet the stringent timing and resource constraints of automotive environments, lightweight cryptographic authentication methods offer a promising balance between security and performance. Cui et al. [63] introduce Payload Processor, an efficient method that integrates Hash-based Message Authentication Code (HMAC) tags into compressed CAN bus frames. Their solution achieves rapid, frame-by-frame authentication with minimal latency (729–1141 μs) and no loss of payload information, positioning it as highly suitable for resource-limited vehicular environments where real-time processing is critical.

Hybrid Cryptographic Solutions. Hybrid cryptographic approaches combine robust encryption techniques with digital signatures to ensure both message confidentiality and authenticity. Park et al. [64] present a security mechanism for CAN bus communications using AES encryption (Electronic Code Book mode) and Elliptic Curve Digital Signature Algorithm (ECDSA) signatures. This dual-layered cryptographic method guarantees secure message confidentiality and robust integrity verification within sub-second processing times, although it relies on a non-standard CAN frame format, potentially complicating integration into existing automotive systems.

These methodologies show a clear trend toward developing resilient and scalable solutions that better protect data integrity within vehicle communication networks.

4.1.5. Comparative analysis

The research on secure communication and data integrity addresses the inherent vulnerabilities of intra-vehicle network protocols, particularly CAN. However, they adopt significantly different strategies, each tackling complementary areas of the security challenge.

Threat Model and Approach: The methods target different types of threats. Oham et al. [22] focus on systemic integrity, using a blockchain framework (B-FERL) to detect unauthorized ECU state changes and provide verifiable forensics, thereby addressing insider threats or deeper system compromises. In contrast, Cui et al. [63] and Park et al. [64] focus on message-level security, employing cryptographic techniques (HMAC and AES/ECDSA, respectively) to prevent spoofing and manipulation of real-time data during bus transmission.

Proactive vs. Reactive Nature: This difference in approach leads to a distinction in their operational nature. The cryptographic solutions offered by Cui et al. [63] and Park et al. [64] are inherently proactive, aiming to prevent successful attacks by ensuring message authenticity and confidentiality from the outset. Oham et al.'s [22] blockchain solution, while providing a strong verification mechanism, is primarily reactive in terms of attack detection, identifying integrity violations after they may have occurred based on recorded state transitions.

Efficiency, Performance, and Validation: Efficiency considerations clearly favour lightweight cryptographic methods, essential for resource-constrained ECUs and real-time operation. Cui et al. [63] report minimal latency overhead (729–1141 μs) for their HMAC-based frame authentication, validating its suitability for embedded environments. Park et al. [64] achieve sub-second processing for AES/ECDSA operations, though their reliance on a non-standard CAN frame format presents compatibility challenges for integration into existing systems. Oham et al.'s [22] B-FERL framework, validated through simulation and comparative evaluations, demonstrates functional efficiency but faces potential latency bottlenecks inherent in blockchain consensus mechanisms, especially when scaling to large vehicle fleets or high transaction volumes. Specific validation details for the cryptographic methods beyond reported latency figures were not available in the provided summaries.

Scalability and Reliability: Scalability appears more challenging for the blockchain-based approach [22] due to potential latency and consensus overhead, whereas the lightweight cryptographic solutions [63,64] are likely more scalable at the message level, though widespread deployment requires careful key management strategies. Reliability, however, is a strong point for all methods: B-FERL ensures reliability through the tamper-resistant and verifiable nature of the blockchain ledger, while the cryptographic methods provide high reliability through robust message authentication and integrity checks.

4.1.6. Synthesis

The reviewed methodologies are complementary: some focus on system-wide trust and validation, while others provide real-time, message-level protection. Blockchain-based approaches are particularly effective for trust management and systemic validation, making them ideal for scenarios that require transparency and accountability. Meanwhile, lightweight cryptographic methods deliver efficient, proactive defenses essential for real-time data exchange. An integrated strategy combining blockchain's system-level security with cryptographic real-time protection offers a promising path to robust intra-vehicle network security. As these solutions evolve, their capacity to maintain data integrity during interface handoffs-such as between internal CAN networks and external V2X systems-will be critical for end-to-end security across the telematics stack.

4.2. V2X communication layer security solutions

Extending connectivity beyond the vehicle, the V2X Communication Layer (Section 3.2) enables crucial safety and efficiency applications by facilitating real-time data exchange with other vehicles, infrastructure, pedestrians, and networks. However, this interaction with the external environment introduces distinct and significant security challenges. The wireless nature of V2X (using DSRC or C-V2X standards) exposes communications to eavesdropping, message injection, and jamming attacks, potentially compromising safety alerts or traffic management data [20,34]. Furthermore, the exchange of potentially sensitive data, which can include location and vehicle identifiers, raises substantial privacy concerns, risking user tracking or profiling if not adequately protected [40,41]. Any security solution must also contend with the high mobility and potential scale of Vehicular Ad Hoc Networks (VANETs), demanding low latency and efficient operation. This subsection delves into security solutions specifically designed for the V2X context, examining approaches aimed at Privacy Preservation (Section 4.2.1) and those focused on ensuring Availability and Resilience against disruptive attacks (Section 4.2.4).

4.2.1. Privacy preservation

Ensuring privacy in V2X communications is essential, as vehicles frequently exchange sensitive positional, behavioral, and operational data with external entities. Privacy-preserving techniques help mitigate the risk of unauthorized tracking, eavesdropping, and data misuse, crucial for user acceptance and regulatory compliance. Recent methodologies leverage federated learning, blockchain technologies, and advanced cryptographic schemes to safeguard data privacy while maintaining efficient, reliable V2X communications.

Solution Summaries.

Federated Learning-based Solutions. Federated learning has emerged as a powerful strategy for ensuring data privacy in decentralized vehicular environments. Lu et al. [33] propose a federated learning scheme tailored for vehicular cyber-physical systems (VCPS). Their method leverages local intelligent data transformations, ensuring sensitive vehicular data remains on-device, thus significantly reducing data leakage risks. Experimental evaluations demonstrate high accuracy and privacy preservation, making this approach well-suited to dynamic V2X scenarios.

Complementing this, Byun et al. [39] introduce a secure aggregation protocol specifically designed for federated learning in vehicular networks using LTE/5G infrastructures. Their system employs pseudonym certificates and robust cryptographic practices to protect against honest-but-curious threats, while significantly reducing communication latency by approximately 11.9% on 5G networks. This solution effectively addresses both privacy and performance demands in high-density vehicular environments.

Blockchain-enhanced Methods. Blockchain technology further reinforces privacy protection through decentralized management and secure data sharing frameworks. Saqib et al. [40] present a blockchain-integrated, group-leader-based shadowing approach for vehicular ad hoc networks (VANETs). By combining k-anonymity with path confusion techniques, their method effectively counters threats of location tracking, significantly enhancing the anonymity set size and overall entropy, thus strengthening location privacy in dynamic vehicular networks.

Blockchain and Zero-Knowledge Proofs for Federated Learning Privacy. Federated learning processes themselves can be vulnerable, particularly to data poisoning attacks where malicious participants submit corrupt model updates. Smahi et al. [65] propose BV-ICVs, a framework using a consortium blockchain and zero-knowledge proofs (zkSNARKs) to verify the integrity of local model updates submitted by vehicles in an FL process without revealing the private training data. This approach aims to ensure the accuracy of the global model while preserving privacy, targeting Byzantine attacks within V2X environments and aiming for scalable verification.

Pseudonym-based Certificate Systems. Innovative certificate management systems using pseudonyms have also gained attention for privacy preservation. Verheul et al. [41] propose IFAL, an efficient certificate management scheme for ETSI ITS frameworks, relying on pre-issued pseudonym certificates activated via short activation codes. IFAL ensures vehicle pseudonym unlinkability, providing robust protection against long-term tracking with minimal bandwidth requirements. The scheme effectively manages privacy and scalability challenges inherent to large-scale V2X deployments.

Behavioral Privacy Preservation. In addition to safeguarding location and identity, more advanced privacy research addresses the challenge of protecting a driver's intrinsic behavioral characteristics. A key example is the work by Zhou and Yang [66], who tackle the inference of a driver's car-following parameters in mixed-autonomy platoons. They propose a parameter privacy filter that allows a vehicle to broadcast statistically distorted, yet plausible, state information, effectively masking the driver's true behavior. This work is notable for formally analyzing the trade-off between the achieved level of privacy and the resulting impact on the platoon's control performance and string stability.

Together, these methodologies represent significant progress in creating reliable, privacy-preserving V2X communication systems. Each approach uniquely balances data confidentiality, communication efficiency, and adaptability to large-scale, heterogeneous vehicular networks.

4.2.2. Comparative analysis

The reviewed privacy-preserving methods for V2X communications illustrate a range of proactive solutions, mainly centered around decentralization as a core strategy, addressing distinct threats and performance considerations within the security landscape of V2X.

Threat Model Focus: The solutions target varied privacy threats. Federated learning approaches primarily focus on preventing sensitive data leakage during distributed model training, explicitly considering honest-but-curious adversaries [33,39] or data poisoning attacks aimed at corrupting the model [65]. Other approaches address location privacy by mitigating tracking and eavesdropping risks through methods such as k-anonymity and path confusion, often strengthened with blockchain integration [40]. Pseudonym-based systems, such as IFAL [41], specifically target long-term vehicle tracking by preventing the association of V2X messages over time. Moving beyond these, the work by Zhou and Yang [66] addresses the more nuanced threat of an adversary inferring a driver's intrinsic behavioral privacy (e.g., their car-following style) from the kinematic data shared in platoon control scenarios.

Proactive Nature: A common characteristic is the proactive stance against privacy violations. Federated learning inherently minimizes data exposure [33,39], while extensions add verifiable integrity checks [65] or secure aggregation [39] before issues arise. Blockchain methods proactively apply anonymity techniques [40], and IFAL proactively manages pseudonym issuance and activation to prevent tracking [41]. The parameter privacy filter proposed by Zhou and Yang [66] also acts proactively, but through a different mechanism of continuous, real-time data distortion, ensuring that the driver's true behavioral model is never directly exposed.

Efficiency and Validation: Efficiency varies, reflecting different optimization goals. IFAL [41] stands out for its bandwidth efficiency (requiring less than one SMS per day for activation codes) and minimal computational overhead, validated via proof-of-concept and formal modeling. Federated learning schemes generally offer efficient decentralized processing; Lu et al. [33] report near-real-time performance based on real-world dataset evaluations, while Byun et al. [39] experimentally demonstrate an 11.9% latency reduction on 5G networks and acceptable computational costs, although noting potentially high server storage needs for large fleets. Blockchain-based solutions offer strong guarantees but can introduce latency; Saqib et al. [40] demonstrate im-

proved anonymity metrics in experimental settings but don't quantify latency overhead, while Smahi et al. [65] aim for efficiency using zk-SNARKs, though specific performance results were not detailed in the summary. The work by Zhou and Yang [66] is distinct in its validation approach, formally analyzing the direct trade-off between privacy and control performance by quantifying the marginal impact of their privacy filter on physical metrics such as fuel consumption and platoon string stability.

Scalability: Decentralized approaches generally offer good scalability. IFAL [41] scales well to large fleets due to its efficient activation mechanism. Federated learning methods [33,39,65] achieve scalability through distributed processing, although performance can depend on network conditions, client participation, and aggregation mechanisms. Blockchain-based solutions, exemplified by Saqib et al. [40], offer moderate scalability depending on the efficiency of their consensus mechanisms. The vehicle-level privacy filter from Zhou and Yang [66] is also inherently scalable, and their proposed learning-based extension is specifically designed to handle continuous parameter spaces efficiently.

Accuracy and Robustness: Methods demonstrate robustness in achieving their specific privacy goals. Federated learning approaches show high accuracy in preserving data privacy during training [33] and can maintain model performance even with a percentage of malicious participants [39]. Blockchain-enhanced methods significantly improve anonymity metrics against tracking [40], while IFAL provides strong, verifiable pseudonym unlinkability [41]. Frameworks that incorporate verification mechanisms such as zkSNARKs improve resilience to data poisoning [65]. The robustness of the approach by Zhou and Yang [66] is demonstrated by its ability to significantly increase an attacker's parameter estimation error (normalized RMSE) while having a minimal and quantifiable impact on vehicle control.

4.2.3. Synthesis

The privacy-preserving techniques examined show a clear progression toward decentralized, efficient, and proactive security tailored to V2X communication's unique vulnerabilities. Federated learning methods, such as those by Lu et al. [33] and Byun et al. [39], offer decentralized privacy with high accuracy and low latency, perfect for real-time vehicular needs. Blockchain-enhanced frameworks, exemplified by Saqib et al. [40], provide strong defenses against tracking and eavesdropping, though they face scalability and latency challenges. Pseudonym management systems, such as IFAL [41], provide scalable and efficient unlinkability with minimal overhead. The emergence of solutions focused on behavioral privacy, such as the parameter privacy filter in Zhou and Yang [66], indicates that the field is maturing to address more subtle threats beyond identity and location. As these privacy solutions advance, their integration with interface-specific measures-such as secure handoffs between V2X and cloud systems-will be essential to safeguard privacy throughout the data flow, particularly at critical transition points in the telematics architecture.

4.2.4. Availability and resilience

V2X communication must remain available and resilient to guarantee reliability, particularly during cyberattacks or network disruptions. Recent studies emphasize a range of techniques to enhance system robustness. These include network-level collaborative approaches such as federated learning and AI-based attack detection, proactive measures such as quantum-resistant cryptography, and vehicle-level adaptive control strategies designed to autonomously validate data and maintain operational stability during an attack.

Solution Summaries.

Federated and Decentralized Methods. Federated and decentralized solutions leverage distributed mechanisms to enhance network resilience and availability. Nakayiza et al. [37] develop a federated learning framework tailored to resource-constrained Vehicular Ad-hoc Networks (VANETs). By adaptively selecting nodes with sufficient resources for participation, their method achieves a 99% detection accuracy for distributed denial-of-service (DDoS) attacks, balancing performance and scalability. Ye et al. [67] propose a decentralized Deep Reinforcement Learning (DRL) framework to optimize resource allocation within Vehicle-to-Vehicle (V2V) communications, effectively enhancing network availability and minimizing latency despite interference, suitable for highly dynamic vehicular environments.

AI and ML-based Detection. ML approaches significantly bolster resilience through rapid and accurate attack detection. Sherazi et al. [42] introduce an IDS using fuzzy logic and Q-learning to robustly detect DDoS attacks in IoV networks, ensuring low overhead and real-time adaptability in resource-limited environments. Krayani et al. [38] present a Generalized Dynamic Bayesian Network (GDBN) paired with a Modified Markov Jump Particle Filter (M-MJPF) for accurate jammer detection in Vehicle-to-Infrastructure (V2I) networks, achieving reliable detection across diverse attack scenarios. Similarly, Ullah et al. [68] employ a hybrid deep neural network to detect RF jamming with 90.4% accuracy in hybrid RF-VLC vehicular communication systems, significantly improving network resilience through precise path-loss estimation.

Proactive Protocols and Cryptographic Solutions. Proactive measures, including protocol optimizations and cryptographic enhancements, directly mitigate vulnerabilities, ensuring network robustness. Twardokus et al. [34] propose lightweight detection techniques against intelligent DoS attacks in 5G Cellular Vehicle-to-Everything (C-V2X) networks, restoring packet delivery rates to over 95% through retransmission and Semi-Persistent Scheduling (SPS) adjustments. Yoshizawa and Preneel [69] focus on cryptographic resilience, introducing hybrid certificates that preserve communication availability amid transitions to quantum-resistant protocols, ensuring long-term resilience in V2X networks.

Resilience through Data Validation. Another key strategy for resilience focuses on validating data at the vehicle level using trusted local sensors. A prime example is the work by Li et al. [70], who propose a reliable cooperative control strategy for vehicular platoons that uses onboard sensors and a statistical chi-squared (χ^2) test to continuously evaluate the reliability of V2V data, adaptively adjusting control inputs to maintain string stability in the presence of data falsification attacks.

4.2.5. Comparative analysis

The surveyed solutions targeting V2X availability and resilience address a diverse set of threats through varied methodologies, generally balancing proactive prevention and mitigation with reactive detection.

Threat Model Focus: A significant cluster of research focuses on defending against DoS attacks, particularly Distributed DoS (DDoS), which can cripple V2X communication. Solutions range from adaptive federated learning frameworks for DDoS detection in resource-constrained VANETs [37], to AI-driven IDS employing methods such as fuzzy logic, Q-learning [42], or LSTM models deployed in edge networks [71]. Another significant threat is signal jamming, with proposed solutions using AI/ML techniques such as Generalized Dynamic Bayesian Networks (GDBN)[38] or hybrid Deep Neural Networks[68] for detection. Alongside these, another critical threat vector is the direct manipulation of V2V data; for example, the falsification or replay attacks addressed by Li et al. [70], which aim to destabilize vehicle platoons by corrupting control-relevant information. Resource contention and inefficient allocation, which implicitly threaten availability, are tackled using decentralized Deep Reinforcement Learning (DRL) [55]. Proactive approaches look towards future threats, including sophisticated intelligent DoS attacks exploiting 5G C-V2X scheduling [34] and the eventual need for quantum-resistant cryptography to maintain availability during cryptographic transitions [69]. Some methods also aim to improve resilience by adapting to emerging, previously unseen attack patterns using transfer learning [72].

Proactive vs. Reactive Approaches: The solutions present a balanced mix. Federated learning [37,71] and decentralized DRL [55] often incorporate proactive elements by optimizing resource use or dis-

tributing detection capabilities preemptively. Protocol-level enhancements [34] and future-proofing cryptographic standards [69] are inherently proactive. Conversely, many AI-based detection systems operate reactively, identifying attacks such as DDoS or jamming as they occur [38,42,68,72], enabling rapid response and mitigation. The work by Li et al. [70] represents a third, hybrid paradigm: a real-time adaptive control system. Rather than simply detecting an attack (reactive) or preventing it beforehand (proactive), their solution continuously evaluates data reliability and adapts the vehicle's control law, offering a constant state of resilience. Twardokus et al. [34] combine reactive detection with proactive mitigation strategies.

Efficiency and Scalability: Federated learning [37,71] and decentralized DRL [55] are often highlighted for their scalability potential in large, dynamic vehicular networks, distributing computational load and preserving privacy. Proactive protocol adjustments [34] and cryptographic solutions [69] are designed with efficiency and long-term scalability in mind. The efficiency of AI-driven detection systems varies; some explicitly target resource-constrained environments [42], while others may involve trade-offs between detection complexity and computational overhead [68]. In contrast, the approach used by Li et al. [70] is noted for its computational efficiency, as the statistical χ^2-test requires less overhead than complex ML models, making it suitable for real-time application in individual vehicle controllers.

Validation and Effectiveness: Validation methods vary widely, encompassing simulations [38,42,55], experiments on specific datasets such as VeReMi-extension [71] and AWID [72], real-world RF/VLC data [68], and evaluations of experimental protocols [34]. High effectiveness is frequently reported: federated learning approaches achieve DDoS detection accuracy around 99% [37] or overall attack detection accuracy of 98.4% [71]; jamming detection accuracy reaches 90.4% in hybrid systems [68]; transfer learning maintains high accuracy (92-96%) even with limited data for new attacks [72]; and proactive mitigations restore packet delivery rates to over 95% against certain DoS attacks [34]. The adaptive control strategy by Li et al. [70] was validated on the NGSIM dataset. Instead of attack detection accuracy, its performance was measured by its ability to maintain platoon string stability and dampen traffic oscillations, demonstrating a focus on physical system resilience. In contrast, proactive strategies such as post-quantum readiness [69] are validated analytically against established standards, focusing on preventing future disruptions rather than detecting present ones.

4.2.6. Synthesis

The reviewed solutions underscore the necessity of blending proactive and reactive strategies to effectively maintain V2X network availability and resilience. As illustrated in Fig. 6, the most robust architectures will likely employ a multi-layered defense, pairing network-wide intelligence with localized, real-time data integrity checks to ensure stability. Network-level collaborative approaches, such as federated learning and decentralized AI, show significant promise for their scalability and swift detection capabilities. At the same time, a recurring theme is the importance of vehicle-level resilience, where trusted onboard sensors are used to autonomously validate external V2X communications. This suggests that the most robust architectures will likely employ a multi-layered defense, pairing network-wide intelligence with localized, real-time data integrity checks to ensure stability. However, notable gaps persist, especially in achieving comprehensive resilience against advanced threats such as sophisticated jamming and quantum-based vulnerabilities. Future research should therefore focus on these hybrid, multi-layered defense frameworks that enhance security across the entire V2X ecosystem.

4.3. Interface-specific layer security solutions

While securing the Intra-Vehicle and V2X layers individually is essential, the interfaces connecting these domains, as well as linking them to Cloud/IoT services, represent critical junctures where security guarantees must be maintained across boundaries. As discussed conceptually alongside Cloud/IoT integration (Section 3.3), these interfaces often bridge disparate protocols (e.g., CAN to IP-based networks), architectures, and trust domains. This heterogeneity can create vulnerabilities if data transitions are not handled securely, potentially allowing threats to propagate between layers [73]. Weaknesses at interfaces, such as inadequate authentication during OTA updates originating from the cloud or insecure translation in gateways handling V2X messages destined for internal ECUs, can undermine the security of the entire system [48,49]. Addressing these specific cross-boundary risks requires dedicated solutions. This subsection examines mechanisms that secure critical integration points, including Secure Transitions for protecting data integrity across protocol or layer boundaries (Section 4.3.1), and Authentication and Access Control methods essential for interactions such as OTA updates (Section 4.3.4).

4.3.1. Secure transitions

Secure transitions ensure that data remains protected as it moves between different protocols or layers, often facilitated by gateways or specialized networking methods.

Solution Summaries.

Gateway-based Security. Gateway-based approaches focus on securing data transitions through dedicated hardware or software gateways. Park et al. [73] propose a secure gateway for routing data between CANFD and Ethernet networks, using CMAC with AES-128 to ensure integrity and defend against threats such as tampering and unauthorized access.

Networking Protocol Enhancements. Networking protocol enhancements aim to secure transitions by integrating security into the communication protocols themselves. Lee et al. [74] introduce an interconnection methodology that extends Time-Sensitive Networking (TSN) with V2X communication, leveraging IEEE 802.11p and synchronized grandmasters to ensure secure and timely data flow from intra-vehicle networks to V2X, reducing end-to-end delays to less than 100 μs. Similarly, Threet et al. [75] present a Named Data Networking (NDN) approach with digital signatures to secure communication across CAN, LIN, and Ethernet protocols, unifying data flow with built-in security to prevent masquerading and replay attacks through signature validation.

Wireless Interface Analysis. Renganathan et al. [49] investigate vulnerabilities in Bluetooth-enabled infotainment systems, focusing on scenarios where a temporary handover of the vehicle (e.g., to a valet) can expose residual data such as phonebook entries. Using a system-theoretic process analysis (STPA-Priv), they mapped the risks that arise from automatic pairing and minimal reconnection prompts. Their work identified specific threats, including silent reconnection and OS-level exploits. To counter these, they proposed design-time mitigations such as refined permission gates and robust re-authentication, which they validated through proof-of-concept demonstrations.

4.3.2. Comparative analysis

The comparative analysis of secure transition solutions reveals diverse strategies tailored to safeguard data flow across different types of interfaces within the broader telematics architecture.

Threat Model: The studies collectively address a spectrum of threats specific to interface points. Park et al. [73] focus on data tampering and unauthorized access at the gateway bridging CANFD and Ethernet. Lee et al. [74] primarily tackle timing delays and ensuring reliable safety message delivery during intra-vehicle TSN to V2X transitions. Threet et al. [75] tackle network-level threats such as masquerading and replay attacks across various protocols (CAN, LIN, Ethernet) using NDN. Renganathan et al. [49], shifting focus to wireless interfaces, highlight unauthorized access and privacy breaches involving residual data in Bluetooth-connected infotainment systems during temporary han-

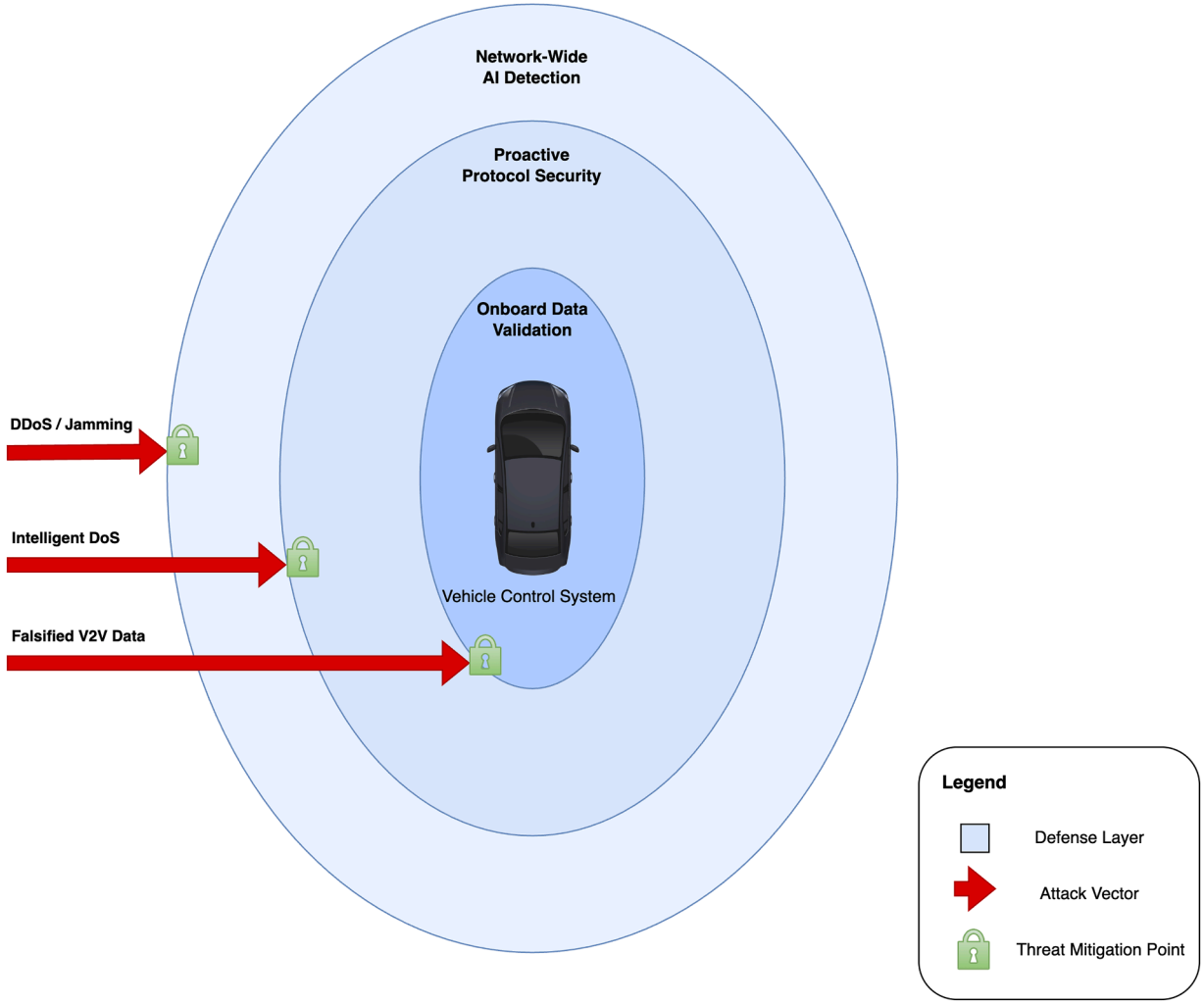


Fig. 6. A "Defense-in-Depth" security model for V2X resilience. Threats are addressed at multiple layers: large-scale network attacks, such as DDoS and jamming, are managed by **Network-Wide AI Detection**[38,42]; protocol-level issues are tackled by **Proactive Protocol Security**[34]; and manipulated messages, including **Falsified V2V Data**, are screened by **Onboard Data Validation** using trusted local sensors before impacting vehicle control [70].

dovers. This diversity underscores the necessity of interface-specific security measures.

Proactive vs. Reactive: A commonality among the reviewed solutions is their proactive nature, aiming to prevent security failures before they occur. Park et al. [73] employ cryptographic integrity checks within the gateway. Lee et al. [74] utilize protocol synchronization (TSN and IEEE 802.11p) for timely delivery. Threet et al. [75] leverage NDN's inherent security features such as mandatory data signing. Renganathan et al. [49] propose design-time mitigations derived from systematic process analysis. This emphasis reflects the criticality of preventing breaches at potentially vulnerable transition points.

Efficiency and Validation: Performance impact, particularly latency, varies significantly. Lee et al.'s [74] iTSN design targets ultra-low latency ($< 100\mu s$), crucial for V2X safety messages, although this figure stems from the proposed methodology awaiting full simulation validation. Park et al. [73] provide concrete latency measurements (433–475 μs for secure methods) from a test environment evaluation, quantifying the overhead of CMAC verification in a gateway. Threet et al. [75] also report measured latency overheads (28.4–38.9 ms, depending on caching) from their Raspberry Pi testbed validation, indicating a higher delay associated with the NDN signing and verification process that might challenge some real-time operations. Renganathan et al. [49], focusing on design-time analysis via STPA-Priv validated with proof-of-concept demonstrations, do not provide runtime efficiency metrics but emphasize preventing vulnerabilities early in the development cycle.

Scalability: Protocol-based solutions generally offer higher scalability. The TSN extensions proposed by Lee et al. [74] and the NDN framework by Threet et al. [75] are designed to operate across multiple interconnected systems. In contrast, gateway-specific approaches, such as Park's [73], require implementation at each gateway. The success of Renganathan's [49] mitigations also hinges on consistent deployment across infotainment systems.

Compatibility: Compatibility with existing automotive systems is a key differentiator. Approaches building on existing standards or processes, such as secure gateways integrating CMAC [73], TSN extensions [74], or design-time analysis [49], generally offer higher compatibility. The NDN paradigm proposed by Threet et al. [75], while offering inherent security benefits, represents a significant departure from current IP-based networking and thus faces greater adoption hurdles due to lower compatibility with existing infrastructure.

4.3.3. *Synthesis*

Our analysis of secure transition solutions shows a clear trend toward proactive, interface-specific security that addresses the challenges of data flow across telematics systems. A key trend is the integration of security into existing protocols, as demonstrated by Lee et al. [74] and

Park et al. [73], which offer high compatibility and low to moderate latency, critical for real-time operations, while Threet et al. [75] introduce the innovative NDN paradigm with strong scalability despite its compatibility challenges. Renganathan et al. [49] fill a vital gap by focusing on wireless interfaces, emphasizing privacy-centric design-time mitigations for Bluetooth vulnerabilities. However, a significant limitation remains the limited attention to V2X-to-cloud transitions, with most solutions targeting intra-vehicle or V2X interfaces. Future research should explore hybrid approaches that combine protocol enhancements (e.g., TSN, NDN) with systematic interface analysis (e.g., STPA-Priv), potentially developing standardized frameworks to ensure secure, scalable transitions across all interface types, including cloud interactions.

4.3.4. Authentication and access control

Authentication and access control ensure that only authorized entities access or update systems across the Interface-Specific Layer, particularly during OTA firmware updates between cloud servers and IVNs. This subsection focuses on safeguarding data integrity and confidentiality, addressing challenges such as real-time performance, fleet-wide scalability, and secure handoffs across interfaces. Using cryptographic and systematic methods, these solutions mitigate risks such as tampering and unauthorized firmware deployment. This analysis evaluates recent advancements, highlighting effective strategies and identifying gaps for future research.

Solution Summaries. The following solutions address authentication and access control challenges in securing OTA firmware updates, ensuring data integrity and authorized access across the Interface-Specific Layer.

Multi-Trust Signature-Based Authentication. Mbakoyiannis et al. [76] propose a secure firmware-over-the-air (FOTA) framework that leverages multi-trust signatures, specifically ED25519, combined with timestamp validation to authenticate OTA updates from cloud servers to intra-vehicle ECUs. This method ensures that only verified updates are deployed, achieving a 100% detection rate for tampering attempts while maintaining minimal latency, making it well-suited for real-time automotive applications.

Attribute-Based Encryption for Access Control. Ghosal et al. [48] introduce STRIDE, a secure OTA update mechanism that employs ciphertext-policy attribute-based encryption (CP-ABE) to enforce fine-grained access control. By ensuring that only authorized vehicles with the correct attributes can decrypt and install firmware updates, STRIDE reduces computational overhead by 52%, providing a scalable and efficient solution tailored to large vehicle fleets while balancing security and performance.

4.3.5. Comparative analysis

The authentication and access control solutions proposed by Mbakoyiannis et al. [76] and Ghosal et al. [48] offer complementary cryptographic approaches to securing a critical interface: the OTA firmware update process between cloud servers and IVNs.

Threat Model and Validation: Both address crucial OTA threats, but with different emphases. Mbakoyiannis et al. [76] focus primarily on ensuring firmware integrity and authenticity, specifically preventing tampering during the update. Their prototype validation demonstrated effectiveness, achieving a 100% detection rate for tampering attempts such as hash mismatches. Ghosal et al. [48], conversely, prioritize preventing unauthorized access to updates, ensuring only vehicles meeting specific criteria (attributes) can decrypt and install firmware, while also considering threats such as DoS and rollback attacks. Their validation involved experimental comparisons against state-of-the-art solutions and proof-of-concept implementation under real-world scenarios.

Authentication and Access Control Mechanism: Reflecting their threat focus, the mechanisms differ. Mbakoyiannis et al. [76] employ multi-trust signatures (specifically ED25519) combined with timestamp validation to verify the source and freshness of the update package. Ghosal et al. [48] utilize ciphertext-policy attribute-based encryption (CP-ABE), enabling fine-grained access control where decryption keys are tied to vehicle attributes managed by the OEM, thus restricting installation to authorized recipients only.

Efficiency and Performance: Both solutions consider performance crucial for OTA. Mbakoyiannis et al. [76] report manageable computational latency, with signature verification taking approximately 48ms in their prototype implementation, suitable for many ECU contexts. Ghosal et al. [48] emphasize efficiency gains achieved through their CP-ABE scheme and dynamic scheduling algorithm, reporting significant reductions of over 52% in computation and storage overhead compared to benchmarks in their experimental validation, along with improvements in propagation delay and throughput.

Scalability: Scalability for large, diverse vehicle fleets is a key consideration for OTA. Ghosal et al. [48] explicitly design STRIDE with scalability in mind, leveraging the policy flexibility of CP-ABE and optimized scheduling to handle millions of vehicles. Mbakoyiannis et al. [76] address scalability through the efficiency of their chosen cryptographic primitives (ED25519) and overall framework design, aiming for minimal overhead suitable for broad deployment.

Compatibility: Integration with existing telematics infrastructure is feasible for both. Mbakoyiannis's signature-based approach aligns well with standard firmware verification practices. Ghosal's attribute-based system might require more significant infrastructural setup for managing attributes and policies compared to simpler signature schemes, potentially impacting initial deployment complexity.

4.3.6. Synthesis

The analysis of authentication and access control solutions for the Interface-Specific Layer highlights a strategic shift toward efficient, scalable security for OTA firmware updates, leveraging cryptographic techniques to ensure integrity and access control. Mbakoyiannis et al. [76] demonstrate the strength of multi-trust signatures in achieving high integrity with minimal latency, while Ghosal et al. [48] showcase the scalability of attribute-based encryption for large fleets. A notable gap lies in the absence of dynamic key management frameworks to adapt to evolving interface security requirements, limiting flexibility across diverse deployments. Future research should focus on developing adaptive authentication protocols that integrate real-time key rotation with attribute-based systems, enhancing resilience against emerging threats and ensuring robust security across all interface interactions.

4.4. Conclusion of the analysis of data flow security

Our analysis shows that the Intra-Vehicle, V2X, and Interface-Specific Layers are all critical points for securing the entire telematics data flow. Within the Intra-Vehicle Layer, hybrid IDS and integrated cryptographic-blockchain solutions effectively address internal vulnerabilities, balancing real-time detection with resource constraints. The V2X Communication Layer leverages decentralized methods, such as federated learning and blockchain, to ensure privacy preservation and resilience, though challenges persist in countering advanced threats such as jamming and quantum vulnerabilities. The Interface-Specific Layer employs proactive, tailored measures-such as the secure gateways and cryptographic authentication visually summarized in Fig. 7-to protect transitions across interfaces, with notable gaps in securing V2X-to-cloud interactions and dynamic key management. Collectively, these layers reveal a trend toward decentralized, proactive, and hybrid security solutions that balance efficiency, scalability, and robustness. While significant progress has been made in fortifying telematics systems, ongoing research remains essential to address the evolving threat landscape and ensure the continued safety and reliability of connected and autonomous vehicles.

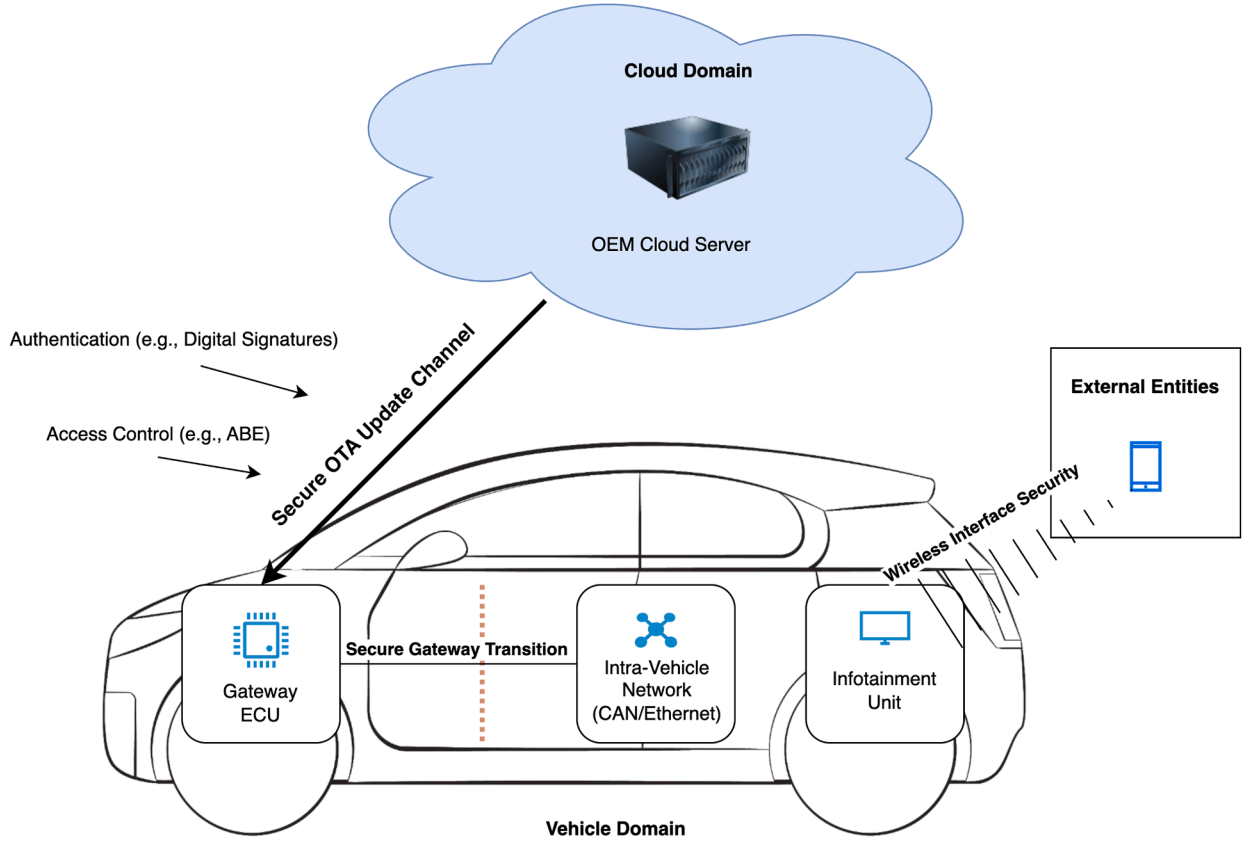


Fig. 7. A model of security solutions applied at critical automotive interfaces. The diagram illustrates distinct mechanisms for: (1) securing the Cloud-to-Vehicle channel for OTA updates through authentication [76] and access control [48]; (2) protecting data transitions at the internal vehicle gateway [73]; and (3) analyzing security for external wireless interfaces such as Bluetooth [49].

5. Discussion

5.1. Key findings and cross-layer trends

Our cross-layer analysis of data flow security maps out key vulnerabilities and solutions, addressing the gap in integrated cybersecurity frameworks that prior research has identified [4,5,8].

Layer-Specific Advancements. For the Intra-Vehicle Layer, hybrid IDS integrating lightweight statistical methods with ML techniques-such as those by Chougule et al. [31] achieving 99.5% accuracy-effectively counter spoofing and DoS attacks on CAN buses. In addition, solutions such as the blockchain-based B-FERL framework and various lightweight cryptographic methods help ensure data integrity and ECU trustworthiness, mitigating risks that could otherwise propagate outwards. In the V2X Communication Layer, decentralized methods emerge as pivotal. Federated learning frameworks [33,37] safeguard sensitive data exchanges with high accuracy (e.g., 99% DDoS detection [37]) without compromising performance. Blockchain-enhanced solutions [40] bolster privacy, while proactive protocols [34] enhance resilience, restoring packet delivery rates above 95% against intelligent DoS attacks. Within the Interface-Specific Layer, secure transition mechanisms, including TSN extensions, achieve sub-100 μs latency, while robust authentication frameworks such as STRIDE provide efficient OTA updates (reducing overhead by 52%).

Emergent Cross-Layer Trends. Synthesizing these layer-specific findings, several overarching trends become apparent, fulfilling our objective to provide a comprehensive view:

- **Shift Towards Proactive and Integrated Security:** Beyond reactive IDS, there is a clear move towards built-in security through cryptographic authentication [63,76], privacy-by-design techniques (FL, pseudonyms [33,41]), and secure interface protocols [73,74].
- **Rise of Decentralization:** Especially in V2X and for ECU integrity, decentralized approaches (blockchain, FL [22,37,40]) are increasingly favored for their potential in privacy and resilience, despite ongoing scalability challenges.
- **Pervasive Role of AI/ML:** AI/ML significantly enhances detection capabilities [19,31,42], but introduces trade-offs regarding efficiency, data dependency [24], and adversarial robustness [30].
- **Interface Security as a Critical Bottleneck:** Securing data handoffs across heterogeneous protocols [73,75] is vital yet complex, representing a key vulnerability nexus where breaches can cascade between layers. For example, the reliability evaluation mechanism [70] operates directly at the V2X interface. It works to ensure that malicious data does not compromise the intra-vehicle control system.

These four emergent trends collectively form our proposed **Cross-Layer Telematics Security Framework**. This framework advocates for: (1) proactive, built-in security through cryptographic authentication and privacy-by-design; (2) decentralized trust models using blockchain and federated learning; (3) AI/ML-enhanced detection balanced with efficiency and adversarial robustness; and (4) prioritized interface security to prevent cross-layer threat propagation. This integrated approach, visualized through our architectural model (Fig. 1) and gap analysis (Fig. 2), addresses the fragmentation identified in prior surveys (Table 1) by providing a unified lens for securing data flows across the entire telematics stack. By consolidating these diverse strategies, the framework offers a cohesive defense against cascading threats that exploit inter-layer vulnerabilities [5,8].

5.2. Implications for vehicle safety, privacy, and industry

Our findings have significant implications for vehicle safety, privacy, and the industry's adoption of new security measures. By securing data flows across layers, integrated solutions enhance the integrity of safety-critical systems (braking, ADAS), directly reducing risks exemplified by the 2015 Jeep hack [2]. Privacy-preserving V2X methods, such as federated learning [33], help prevent data exposure incidents such as the Subaru Starlink breach [1], bolstering user trust. Robust interface security for OTA updates [48,76] is critical to preserving reliability as vehicle connectivity surges towards the projected 95% of new cars by 2030 [3]. On a larger scale, these implications extend to the resilience of the entire transportation network, where regional cyberattacks can trigger macroscopic congestion events. Their significance emphasizes the value of integrated, network-level defense strategies, such as the two-layer control framework proposed by Wang et al. [77], which coordinates local and perimeter traffic control to manage the system-wide impact of an attack.

These technical advancements inform industry practices and standardization. The efficacy of decentralized frameworks may influence evolving standards (e.g., for C-V2X security or secure OTA protocols). Adoption challenges exist, including the resource limits of ECUs for complex ML deployment and the need to improve scalability for blockchain approaches in dense V2X environments [32]. Regulatory bodies can leverage holistic frameworks such as the one presented here to mandate comprehensive, cross-layer security testing and verification. While rapid industry responses, such as Subaru's patch, demonstrate reactive capacity, the proactive measures in this survey offer a path toward incident prevention. Adopting these integrated security strategies is essential for building a safer and more trustworthy connected vehicle ecosystem.

5.3. Limitations and challenges

Despite the progress surveyed, limitations remain, reflecting both this study's scope and broader telematics security challenges. A significant gap, noted in our Gap Identification (Section 2), is the lack of extensive real-world validation for many proposed solutions, particularly ML-based IDS [31], which are often evaluated only on benchmark datasets [24,29]. This limits confidence in their generalizability across diverse operational conditions.

Furthermore, V2X-to-Cloud interactions remain relatively underexplored compared to intra-vehicle or V2X-specific security. This echoes limitations observed in prior surveys [8]. As a result, threats such as large-scale DoS attacks against cloud infrastructure are not sufficiently addressed [42]. While interface solutions exist, securing dynamic wireless interfaces such as Bluetooth often relies on design-time analysis [49] rather than robust run-time mechanisms. Scalability remains a critical challenge, especially for V2X communication in dense urban scenarios [34] and for computationally intensive methods on resource-constrained ECUs [32]. In other words, while the 'cross-layer' security approach [4] is a helpful concept, it still needs to be tested in real-world situations and more thoroughly combined with existing systems to be truly effective.

5.4. Future research directions

Addressing the identified gaps requires targeted future research:

1. **Integrated Cross-Layer Frameworks and Protocols:** Developing and standardizing security architectures that explicitly manage trust and data flow across Intra-Vehicle, V2X, and Cloud/IoT boundaries, potentially integrating TSN principles [74] with secure V2X and cloud interface protocols.
2. **Quantum-Resistant Telematics:** Proactively integrating and standardizing post-quantum cryptography (PQC) across all telematics layers, building on initial V2X explorations [69], to ensure long-term security against emerging threats.
3. **Realistic Large-Scale Validation:** Future work should create comprehensive, cross-layer benchmark datasets that go beyond current offerings [24,29,61,62]. These should be validated through extensive real-world testing or high-fidelity simulations in diverse environments.
4. **Efficient, Robust, and Explainable AI/ML:** Advancing AI/ML for security by focusing on lightweight models suitable for ECUs and enhancing robustness against adversarial attacks. This includes developing defense-aware frameworks, such as the reinforcement learning approach [56] that can train trustworthy policies resilient to worst-case sensor perturbations. Furthermore, incorporating explainable AI (XAI) is critical to increase trust and facilitate debugging.
5. **Scalable Decentralized Systems:** Improving the performance, scalability, and governance models for blockchain and federated learning in high-density, dynamic vehicular networks.
6. **Human-Centric Privacy and Security:** Integrating technical security mechanisms with user-centric privacy controls and considerations [16], ensuring solutions are not only secure but also align with user expectations and societal values.
7. **Integrated Vehicle-to-Network Defenses:** Exploring the integration of vehicle-centric security measures with macroscopic traffic management systems to create coordinated defenses against the network-wide impacts of cyberattacks, building on frameworks such as the two-layer control strategy proposed by Wang et al. [77].

5.5. Concluding remarks

This survey addresses a critical gap in telematics security research: the fragmented treatment of Intra-Vehicle, V2X, and Cloud/IoT layers in prior work (Table 1). Our contributions directly map identified gaps to findings.

First, we counter fragmented approaches with cross-layer analysis. Hybrid IDS such as HybridSecNet achieve 99.5% detection accuracy on CAN buses. Federated learning frameworks attain 99% DDoS detection in V2X communications without compromising privacy. These results confirm that effective telematics security requires coordinated mechanisms across all layers.

Second, we examine interface security, an area prior surveys largely overlooked. Data handoffs between layers present critical vulnerabilities. TSN extensions achieve sub-100 μs latency for secure transitions. STRIDE-based frameworks reduce OTA update overhead by 52%. Such mechanisms are essential for preventing cross-layer threat propagation.

Third, we assess privacy-preserving AI/ML techniques for V2X deployment. Federated learning [33] and pseudonym schemes [41] enable accurate threat detection while protecting user data. These approaches address the tension between security monitoring and privacy.

Taken together, these findings form our Cross-Layer Telematics Security Framework (Section 5). Four trends emerge: proactive security integration, decentralized trust, AI/ML-enhanced detection, and prioritized interface protection. Securing connected vehicles will ultimately require technical innovation, real-world validation, and industry collaboration on standards.

CRediT authorship contribution statement

Junjie Wu: Writing – review & editing, Writing – original draft, Methodology, Conceptualization; **Benjamin C. M. Fung:** Writing – review & editing, Supervision, Project administration, Funding acquisition; **Natalia Stakhanova:** Writing – review & editing, Funding acquisition; **Faiyaz Khan:** Writing – review & editing, Conceptualization; **Hanbo Yu:** Writing – review & editing.

Data availability

No data was used for the research described in the article.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the author(s) used Gemini (a large language model developed by Google) in order to improve the language, readability, and overall clarity of the manuscript. After using this tool, the author(s) reviewed and edited the content as needed and take full responsibility for the content of the published article.

Authorship Declaration

1. I declare that the list of authors on the submission page matches the list of authors in the manuscript. I understand the paper can be rejected or withdrawn if there is a mismatch between the two lists of authors.

2. I declare that there has been no change of authors from the original submission. I understand the paper can be rejected or withdrawn if the list of authors is different from the original submission.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

This research is supported by the National Cybersecurity Consortium (NCC 2023-R8), NSERC Discovery Grants (RGPIN-2024-04087), and Canada Research Chairs Program (CRC-2019-00041).

References

[1] A. Greenberg, Subaru security flaws exposed its system for tracking millions of cars, Wired (2025). Section: tags, https://www.wired.com/story/subaru-location-tracking-vulnerabilities/.

[2] Q. Luo, J. Liu, Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions, IEEE Wireless Commun. 25 (6) (2018) 113–119. Conference Name: IEEE Wireless Communications, https://doi.org/10.1109/MWC.2018.1700364

[3] M. Bertoncello, C. Martens, T. Schneiderbauer, K. Zedelius, Unlocking connected cars with corporate business building | McKinsey, 2023. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/corporate-business-building-to-unlock-value-in-automotive-connectivity.

[4] Y. Wang, Y. Wang, H. Qin, H. Ji, Y. Zhang, J. Wang, A systematic risk assessment framework of automotive cybersecurity, Automot. Innov. 4 (3) (2021) 253–261. https://doi.org/10.1007/s42154-021-00140-6

[5] C.V. Kifor, A. Popescu, Automotive cybersecurity: a survey on frameworks, standards, and testing and monitoring technologies, Sensors 24 (18) (2024) 6139. https://doi.org/10.3390/s24186139

[6] A. Anwar, A. Anwar, L. Moukahal, M. Zulkernine, Security assessment of in-vehicle communication protocols, Veh. Commun. 44 (2023) 100639. https://doi.org/10.1016/j.vehcom.2023.100639

[7] R. Soundarapandiyan, D. Venkatachalam, A. Selvaraj, Real-time data analytics in connected vehicles: enhancing telematics systems for autonomous driving and intelligent transportation systems, Australian J. Mach. Learn. Res. Appl. 3 (1) (2023) 420–460. https://ajmlra.org/index.php/publication/article/view/22.

[8] H. Taslimasa, S. Dadkhah, E.C.P. Neto, P. Xiong, S. Ray, A.A. Ghorbani, Security issues in internet of vehicles (IoV): a comprehensive survey, Internet of Things 22 (2023) 100809. https://doi.org/10.1016/j.iot.2023.100809

[9] L. Wouters, B. Gierlichs, B. Preneel, My other car is your car: compromising the tesla model x keyless entry system, IACR Trans. Cryptographic Hardw. Embedded Syst. (2021) 149–172. https://doi.org/10.46586/tches.v2021.i4.149-172

[10] Z. Zhang, Y. Zhang, J. Zhang, J. Xie, S. Liu, An endogenous security study of telematics box in intelligent connected vehicles, IEEE Embed. Syst. Lett. 16 (4) (2024) 501–504. Conference Name: IEEE Embedded Systems Letters, https://doi.org/10.1109/LES.2024.3432593

[11] B. Gul, F. Ertam, In-vehicle communication cyber security: a comprehensive review of challenges and solutions, Veh. Commun. 50 (2024) 100846. https://doi.org/10.1016/j.vehcom.2024.100846

[12] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, K. Li, A survey of intrusion detection for in-vehicle networks, IEEE Trans. Intell. Transp. Syst. 21 (3) (2020) 919–933. https://doi.org/10.1109/TITS.2019.2908074

[13] P.M. Rao, S. Jangirala, S. Pedada, A.K. Das, Y. Park, Blockchain integration for IoT-enabled V2X communications: a comprehensive survey, security issues and challenges, IEEE Access 11 (2023) 54476–54494. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2023.3281844

[14] I. Pali, R. Amin, M. Abdussami, Autonomous vehicle security: current survey and future research challenges, Secur. Priv. 7 (3) (2024) e367. https://doi.org/10.1002/spy2.367

[15] S.M.M. Hossain, S. Banik, T. Banik, A.M. Shibli, Survey on Security Attacks in Connected and Autonomous Vehicular Systems, 2023. arXiv:2310.09510 [cs].

[16] V. Rishiwal, U. Agarwal, A. Alotaibi, S. Tanwar, P. Yadav, M. Yadav, Exploring secure V2X communication networks for human-centric security and privacy in smart cities, IEEE Access 12 (2024) 138763–138788. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2024.3467002

[17] E. Farsimadan, L. Moradi, F. Palmieri, A review on security challenges in V2X communications technology for VANETs, IEEE Access (2025) 1. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2025.3541035

[18] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, J. Alonso-Zarate, A comprehensive survey of V2X cybersecurity mechanisms and future research paths, IEEE Open J. Commun. Soc. 4 (2023) 325–391. Conference Name: IEEE Open Journal of the Communications Society, https://doi.org/10.1109/OJCOMS.2023.3239115

[19] H.M. Song, J. Woo, H.K. Kim, In-vehicle network intrusion detection using deep convolutional neural network, Veh. Commun. 21 (2020) 100198. https://doi.org/10.1016/j.vehcom.2019.100198

[20] T. Yoshizawa, D. Singelée, J.T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, B. Preneel, A survey of security and privacy issues in V2X communication systems, ACM Comput. Surv. 55 (9) (2023) 1–36. https://doi.org/10.1145/3558052

[21] A. Waheed, M.A. Shah, S.M. Mohsin, A. Khan, C. Maple, S. Aslam, S. Shamshirband, A comprehensive review of computing paradigms, enabling computation offloading and task execution in vehicular networks, IEEE Access 10 (2022) 3580–3600. Conference Name: IEEE Access, https://doi.org/10.1109/ACCESS.2021.3138219

[22] C. Oham, R.A. Michelin, R. Jurdak, S.S. Kanhere, S. Jha, B-FERL: Blockchain based framework for securing smart vehicles, Inf. Process. Manag. 58 (1) (2021) 102426. https://doi.org/10.1016/j.ipm.2020.102426

[23] W. Liu, G. Qin, L. Yang, Y. Liang, Flow monitoring alarm module application for in-vehicle CAN bus networks, in: S.S. Yuriy, A. Nayyar (Eds.), 7Th International Conference on Computing, Control and Industrial Engineering (CCIE 2023), Springer Nature, Singapore, 2023, pp. 773–780. https://doi.org/10.1007/978-981-99-2730-2_73

[24] E.C.P. Neto, H. Taslimasa, S. Dadkhah, S. Iqbal, P. Xiong, T. Rahman, A.A. Ghorbani, CICIoV2024: advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus, Internet of Things 26 (2024) 101209. https://doi.org/10.1016/j.iot.2024.101209

[25] A. Martínez-Cruz, K.A. Ramírez-Gutiérrez, C. Feregrino-Uribe, A. Morales-Reyes, Security on in-vehicle communication protocols: issues, challenges, and future research directions, Comput. Commun. 180 (2021) 1–20. https://doi.org/10.1016/j.comcom.2021.08.027

[26] J. Wei, K. Ma, C. Kong, Research on intelligent detection method of automotive network data security based on flexray/CAN gateway, in: Y. Xu, H. Yan, H. Teng, J. Cai, J. Li (Eds.), Machine Learning for Cyber Security, Springer Nature Switzerland, Cham, 2023, pp. 394–408. https://doi.org/10.1007/978-3-031-20096-0_30

[27] J. Clancy, D. Mullins, B. Deegan, J. Horgan, E. Ward, C. Eising, P. Denny, E. Jones, M. Glavin, Wireless access for V2X communications: research, challenges and opportunities, IEEE Commun. Surv. Tut. 26 (3) (2024) 2082–2119. Conference Name: IEEE Communications Surveys & Tutorials, https://doi.org/10.1109/COMST.2024.3384132

[28] S. Jeong, B. Jeon, B. Chung, H.K. Kim, Convolutional neural network-based intrusion detection system for AVTP streams in automotive ethernet-based networks, Veh. Commun. 29 (2021) 100338. https://doi.org/10.1016/j.vehcom.2021.100338

[29] B. Lampe, W. Meng, Can-train-and-test: a curated CAN dataset for automotive intrusion detection, Comput. Secur. 140 (2024) 103777. https://doi.org/10.1016/j.cose.2024.103777

[30] I. Zenden, H. Wang, A. Iacovazzi, A. Vahidi, R. Blom, S. Raza, On the resilience of machine learning-based IDS for automotive networks, in: 2023 IEEE Vehicular Networking Conference (VNC), 2023, pp. 239–246. https://doi.org/10.1109/VNC57357.2023.10136285

[31] A. Chougule, I. Kulkarni, T. Alladi, V. Chamola, F.R. Yu, Hybridsecnet: in-vehicle security on controller area networks through a hybrid two-step LSTM-CNN model, IEEE Trans. Veh. Technol. 73 (10) (2024) 14580–14591. Conference Name: IEEE Transactions on Vehicular Technology, https://doi.org/10.1109/TVT.2024.3413849

[32] S. Khandelwal, E. Wadhwa, S. Shreejith, Deep learning-based embedded intrusion detection system for automotive CAN, in: 2022 IEEE 33Rd International Conference on Application-Specific Systems, Architectures and Processors (ASAP), 2022, pp. 88–92. https://doi.org/10.1109/ASAP54787.2022.00023

[33] Y. Lu, X. Huang, Y. Dai, S. Maharjan, Y. Zhang, Federated learning for data privacy preservation in vehicular cyber-physical systems, IEEE Netw. 34 (3) (2020) 50–56. Conference Name: IEEE Network, https://doi.org/10.1109/MNET.011.1900317

[34] G. Twardokus, H. Rahbari, Toward protecting 5G sidelink scheduling in c-V2X against intelligent DoS attacks, IEEE Trans. Wireless Commun. 22 (11) (2023) 7273–7286. Conference Name: IEEE Transactions on Wireless Communications, https://doi.org/10.1109/TWC.2023.3249665

[35] M. Hasan, S. Mohan, T. Shimizu, H. Lu, Securing vehicle-to-everything (V2X) communication platforms, IEEE Trans. Intell. Veh. 5 (4) (2020) 693–713. Conference Name: IEEE Transactions on Intelligent Vehicles, https://doi.org/10.1109/TIV.2020.2987430

[36] FCC Modernizes 5.9 GHz Band to Improve Wi-Fi and Automotive Safety | Federal Communications Commission, 2020. https://www.fcc.gov/document/fcc-modernizes-59-ghz-band-improve-wi-fi-and-automotive-safety-0.

[37] H.L. Nakayiza, L.A. Chijioke Ahakonye, D.-S. Kim, J.M. Lee, Resource-aware adaptive federated learning for enhanced DDos detection in vehicular ad hoc networks, in: 2024 15Th International Conference on Information and Communication Technology Convergence (ICTC), 2024, pp. 1262–1267. https://doi.org/10.1109/ICTC62082.2024.10826874

[38] A. Krayani, N.J. William, L. Marcenaro, C. Regazzoni, Jammer detection in vehicular V2X networks, in: 2022 Microwave Mediterranean Symposium (MMS), 2022, pp. 1–5. https://doi.org/10.1109/MMS55062.2022.9825566

[39] S. Byun, A. Sarker, S.-Y. Chang, J. Kalita, Secure aggregation for privacy-preserving federated learning in vehicular networks, ACM J. Autonomous Transp. Syst. 1 (3) (2024) 1–25. https://doi.org/10.1145/3657644

[40] N.U. Saqib, S.U.R. Malik, A. Anjum, M.H. Syed, S.A. Moqurrab, G. Srivastava, J.C.-W. Lin, Preserving privacy in internet of vehicles (IoV): a novel group-leader-based shadowing scheme using blockchain, IEEE Internet Things J. 10 (24) (2023) 21421–21430. Conference Name: IEEE Internet of Things Journal, https://doi.org/10.1109/JIOT.2023.3294133

[41] E. Verheul, C. Hicks, F.D. Garcia, IFAL: Issue first activate later certificates for V2X, in: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019, pp. 279–293. https://doi.org/10.1109/EuroSP.2019.00029

[42] H.H.R. Sherazi, R. Iqbal, F. Ahmad, Z.A. Khan, M.H. Chaudary, DDoS attack detection: a key enabler for sustainable communication in internet of vehicles, Sustainable Comput. Inf. Syst. 23 (2019) 13–20. https://doi.org/10.1016/j.suscom.2019.05.002

[43] M.A. Rahim, M.A. Rahman, M.M. Rahman, A.T. Asyhari, M.Z.A. Bhuiyan, D. Ramasamy, Evolution of IoT-enabled connectivity and applications in automotive industry: a review, Veh. Commun. 27 (2021) 100285. https://doi.org/10.1016/j.vehcom.2020.100285

[44] S. Mahmood, H.N. Nguyen, S.A. Shaikh, Systematic threat assessment and security testing of automotive over-the-air (OTA) updates, Veh. Commun. 35 (2022) 100468. https://doi.org/10.1016/j.vehcom.2022.100468

[45] E. Jayatunga, A. Nag, A.D. Jurcut, Security requirements for vehicle-to-everything (V2X) communications integrated with blockchain, in: 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA), 2022, pp. 208–213. https://doi.org/10.1109/BCCA55292.2022.9922372

[46] A. Hbaieb, S. Ayed, L. Chaari, Federated learning based IDS approach for the IoV, in: Proceedings of the 17Th International Conference on Availability, Reliability and Security, ACM, Vienna Austria, 2022, pp. 1–6. https://doi.org/10.1145/3538969.3544422

[47] H. Xiao, W. Zhang, W. Li, A.T. Chronopoulos, Z. Zhang, Joint clustering and blockchain for real-time information security transmission at the crossroads in c-V2X networks, IEEE Internet Things J. 8 (18) (2021) 13926–13938. Conference Name: IEEE Internet of Things Journal, https://doi.org/10.1109/JIOT.2021.3068175

[48] A. Ghosal, S. Halder, M. Conti, Secure over-the-air software update for connected vehicles, Comput. Netw. 218 (2022) 109394. https://doi.org/10.1016/j.comnet.2022.109394

[49] V. Renganathan, E. Yurtsever, Q. Ahmed, A. Yener, Valet attack on privacy: a cybersecurity threat in automotive bluetooth infotainment systems, Cybersecurity 5 (1) (2022) 30. https://doi.org/10.1186/s42400-022-00132-x

[50] A. Boualouache, T. Engel, Federated learning-based inter-slice attack detection for 5G-V2X sliced networks, in: 2022 IEEE 96Th Vehicular Technology Conference (VTC2022-Fall), 2022, pp. 1–6. https://doi.org/10.1109/VTC2022-Fall57202.2022.10012736

[51] J. Cui, F. Ouyang, Z. Ying, L. Wei, H. Zhong, Secure and efficient data sharing among vehicles based on consortium blockchain, IEEE Trans. Intell. Transp. Syst. 23 (7) (2022) 8857–8867. Conference Name: IEEE Transactions on Intelligent Transportation Systems, https://doi.org/10.1109/TITS.2021.3086976

[52] F. Wang, X. Wang, X.J. Ban, Data poisoning attacks in intelligent transportation systems: a survey, Transp. Res. Part C Emerg. Technol. 165 (2024) 104750. https://doi.org/10.1016/j.trc.2024.104750

[53] K.L. Williams, Y.D. Prasanth, M. Jeyaselvi, Hybrid AI architecture using edge-cloud computing for secure V2X communication, in: 2024 9Th International Conference on Communication and Electronics Systems (ICCES), 2024, pp. 913–920. https://doi.org/10.1109/ICCES63552.2024.10859430

[54] P. Mansourian, N. Zhang, A. Jaekel, M. Kneppers, Deep learning-based anomaly detection for connected autonomous vehicles using spatiotemporal information, IEEE Trans. Intell. Transp. Syst. 24 (12) (2023) 16006–16017. https://doi.org/10.1109/TITS.2023.3286611

[55] A. Alfardus, D.B. Rawat, Intrusion detection system for CAN bus in-vehicle network based on machine learning algorithms, in: 2021 IEEE 12Th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2021, pp. 0944–0949. https://doi.org/10.1109/UEMCON53757.2021.9666745

[56] X. He, W. Huang, C. Lv, Trustworthy autonomous driving via defense-aware robust reinforcement learning against worst-case observational perturbations, Transp. Res. Part C Emerg. Technol. 163 (2024) 104632. https://doi.org/10.1016/j.trc.2024.104632

[57] H.M. Song, H.K. Kim, Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data, IEEE Trans. Veh. Technol. 70 (2) (2021) 1098–1108. Conference Name: IEEE Transactions on Vehicular Technology, https://doi.org/10.1109/TVT.2021.3051026

[58] H. Zhang, K. Zeng, S. Lin, Federated graph neural network for fast anomaly detection in controller area networks, IEEE Trans. Inf. Forensics Secur. 18 (2023) 1566–1579. Conference Name: IEEE Transactions on Information Forensics and Security, https://doi.org/10.1109/TIFS.2023.3240291

[59] W. Hao, T. Yang, Q. Yang, Hybrid statistical-machine learning for real-time anomaly detection in industrial cyber-physical systems, IEEE Trans. Autom. Sci. Eng. 20 (1) (2023) 32–46. https://doi.org/10.1109/TASE.2021.3073396

[60] D. Goina, E. Hogea, G. Maties, Enhanced anomaly detection in automotive systems using SAAD: statistical aggregated anomaly detection, in: 2024 26Th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2024, pp. 233–241. https://doi.org/10.1109/SYNASC65383.2024.00046

[61] R.W. van der Heijden, T. Lukaseder, F. Kargl, Veremi: a dataset for comparable evaluation of misbehavior detection in VANETs, in: R. Beyah, B. Chang, Y. Li, S. Zhu (Eds.), Security and Privacy in Communication Networks, Springer International Publishing, Cham, 2018, pp. 318–337. https://doi.org/10.1007/978-3-030-01701-9_18

[62] J. Kamel, M. Wolf, R.W. van der Hei, A. Kaiser, P. Urien, F. Kargl, Veremi extension: a dataset for comparable evaluation of misbehavior detection in VANETs, in: ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, pp. 1–6. https://doi.org/10.1109/ICC40277.2020.9149132

[63] J. Cui, Y. Chen, H. Zhong, D. He, L. Wei, I. Bolodurina, L. Liu, Lightweight encryption and authentication for controller area network of autonomous vehicles, IEEE Trans. Veh. Technol. 72 (11) (2023) 14756–14770. Conference Name: IEEE Transactions on Vehicular Technology, https://doi.org/10.1109/TVT.2023.3281276

[64] C.H. Park, Y. Kim, J.-Y. Jo, A secure communication method for CANBus, in: 2021 IEEE 11Th Annual Computing and Communication Workshop and Conference (CCWC), 2021, pp. 0773–0778. https://doi.org/10.1109/CCWC51732.2021.9376166

[65] A. Smahi, H. Li, Y. Yang, X. Yang, P. Lu, Y. Zhong, C. Liu, BV-ICVs: A privacy-preserving and verifiable federated learning framework for V2X environments using blockchain and zksnarks, J. King Saud Univ. Comput. Inf. Sci. 35 (6) (2023) 101542. https://doi.org/10.1016/j.jksuci.2023.03.020

[66] J. Zhou, K. Yang, A parameter privacy-preserving strategy for mixed-autonomy platoon control, Transportation Research Part C: Emerging Technologies 169 (2024) 104885. https://doi.org/10.1016/j.trc.2024.104885

[67] H. Ye, G.Y. Li, B.-H.F. Juang, Deep reinforcement learning based resource allocation for V2V communications, IEEE Trans. Veh. Technol. 68 (4) (2019) 3163–3173. Conference Name: IEEE Transactions on Vehicular Technology, https://doi.org/10.1109/TVT.2019.2897134

[68] A. Ullah, W. Choi, S. Coleri, Path loss estimation and jamming detection in hybrid RF-VLC vehicular networks: a machine-learning framework, IEEE Sens. J. 23 (24) (2023) 31325–31336. Conference Name: IEEE Sensors Journal, https://doi.org/10.1109/JSEN.2023.3329490

[69] T. Yoshizawa, B. Preneel, Post-quantum impacts on V2X certificates - already at the end of the road, in: 2023 IEEE 97Th Vehicular Technology Conference (VTC2023-Spring), 2023, pp. 1–6. https://doi.org/10.1109/VTC2023-Spring57618.2023.10199793

[70] Z. Li, Y. Zhou, Y. Zhang, X. Li, Enhancing vehicular platoon stability in the presence of communication cyberattacks: a reliable longitudinal cooperative control strategy, Transportation Research Part C: Emerging Technologies 163 (2024) 104660. https://doi.org/10.1016/j.trc.2024.104660

[71] H. Yakan, I. Fajjari, N. Aitsaadi, C. Adjih, Federated learning for V2X misbehavior detection system in 5G edge networks, in: Proceedings of the Int'L ACM Conference on Modeling Analysis and Simulation of Wireless and Mobile Systems, ACM, Montreal Quebec Canada, 2023, pp. 155–163. https://doi.org/10.1145/3616388.3617533

[72] X. Li, Z. Hu, M. Xu, Y. Wang, J. Ma, Transfer learning based intrusion detection scheme for internet of vehicles, Inf. Sci. 547 (2021) 119–135. https://doi.org/10.1016/j.ins.2020.05.130

[73] J.S. Park, D.H. Kim, I.H. Suh, Design and implementation of security function according to routing method in automotive gateway, Int. J. Automot. Technol. 22 (1) (2021) 19–25. https://doi.org/10.1007/s12239-021-0003-9

[74] J. Lee, S. Park, New interconnection methodology of TSNs using V2X communication, in: 2017 IEEE 7Th Annual Computing and Communication Workshop and Conference (CCWC), 2017, pp. 1–6. https://doi.org/10.1109/CCWC.2017.7868447

[75] Z. Threet, C. Papadopoulos, W. Lambert, P. Podder, S. Thanasoulas, A. Afanasyev, S. Ghafoor, S. Shannigrahi, Securing Automotive Architectures with Named Data Networking, 2022. arXiv:2206.08278 [cs].

[76] D. Mbakoyiannis, O. Tomoutzoglou, G. Kornaros, Secure over-the-air firmware updating for automotive electronic control units, in: Proceedings of the 34Th ACM/SIGAPP Symposium on Applied Computing, ACM, Limassol Cyprus, 2019, pp. 174–181. https://doi.org/10.1145/3297280.3297299

[77] L. Wang, H. Ding, N. Zheng, X. Zheng, Two-layer control strategy response to regional cyberattacks on large-scale road networks in a connected vehicle environment, Transp. Res. Part C Emerg. Technol. 174 (2025) 105116. https://doi.org/10.1016/j.trc.2025.105116