information

Article

A Comprehensive Survey of Threats in Platooning—A Cloud-Assisted Connected and Autonomous Vehicle Application

Al Tariq Sheik *, Carsten Maple, Gregory Epiphaniou and Mehrdad Dianati

Warwick Manufacturing Group (WMG), University of Warwick, Coventry CV4 7AL, UK; cm@warwick.ac.uk (C.M.); gregory.epiphaniou@warwick.ac.uk (G.E.); m.dianati@warwick.ac.uk (M.D.)
* Correspondence: t.sheik@warwick.ac.uk

Abstract: Cloud-Assisted Connected and Autonomous Vehicles (CCAV) are set to revolutionise road safety, providing substantial societal and economic advantages. However, with the evolution of CCAV technology, security and privacy threats have increased. Although several studies have been published around the threat and risk estimation aspects of CCAV, limited research exists on the security implications and emerging threat landscapes in the CCAV platooning application. We conducted an extensive review and categorisation of real-world security incidents and created an account of 132 threats from scholarly sources and 64 threats from recorded events in practice. Furthermore, we defined thirty-one (31) trust domains and outlined eight (8) unique attack vectors to supplement existing research efforts for the systematic security analysis of such cyberinfrastructures. Using these findings, we create a detailed attack taxonomy to communicate threat-related information in CCAV and platooning applications and highlight emerging challenges and ways to safeguard the broader CCAV systems. This work acts as a roadmap to existing researchers and practitioners advocating for a 'security and privacy by design' framework for a dynamically evolving CCAV threat landscape.

Keywords: threat analysis; threat landscape; connected vehicles; autonomous vehicles; edge computing; cloud computing; attack taxonomy; threats; attacks; cybersecurity

Citation: Sheik, A.T.; Maple, C.; Epiphaniou, G.; Dianati, M. A Comprehensive Survey of Threats in Platooning—A Cloud-Assisted Connected and Autonomous Vehicle Application. *Information* **2024**, *15*, 14. https://doi.org/10.3390/info15010014

Academic Editors: Vasco N. G. J. Soares, João M. L. P. Caldeira and Jaime Galán-Jiménez

Received: 23 October 2023
Revised: 11 December 2023
Accepted: 12 December 2023
Published: 25 December 2023

1. Introduction

Cloud-Assisted Connected Autonomous Vehicles (CCAVs) are sophisticated cyber-physical systems with significant potential for scientific advancement and business impact. These systems include various elements such as cloud and edge cloud technology, Roadside Units (RSUs), and numerous Connected and Autonomous Vehicles (CAVs) featuring diverse hardware and software platforms. CCAVs aim to enhance road safety, reduce traffic, shorten travel times, optimise distribution logistics, and decrease pollution [1–3]. However, as CCAV technology advances, so does its vulnerability to cyber attacks. This evolving threat landscape means that adversaries can target these systems, making them susceptible to both remote and physical attacks [4–6]. One notable example occurred in 2015, when a cybersecurity flaw led to the recall of 1.4 million vehicles due to a vulnerability in their connectivity systems [7]. Such incidents highlight the range of potential cyber attacks, including Distributed Denial of Service (DDOS), spoofing, information leakage, privilege escalation, and manipulation. Since CCAVs are composed of intricate hardware and software, they present multiple layers of potential vulnerabilities. These vulnerabilities could be exploited through various attack vectors, such as malicious software, impacting the safety-critical functions of the vehicles and potentially harming individuals' safety or organisations' reputation.

Recently, the collaborative driving application among CCAVs known as platooning has been garnering research interest [8]. A platoon refers to a collection of CCAVs that

are travelling in a linear formation within a single lane of a roadway. These vehicles maintain a consistent velocity and are positioned in close proximity to one another, with little spacing between each vehicle [9]. The benefits of platooning include: increased road capacity; decreased traffic congestion; increased safety and comfort; considerably reduced energy consumption and exhaust emissions because of the reduced air resistance across a streamlined platoon; and greater potential for cooperative communication applications through significantly improved vehicular networking performance [10].

Within a platoon, vehicles may take on different roles, including the lead CCAV, a member CCAV, and a joining/leaving CCAV [11]. Lead vehicles are driven semi-autonomously until a platoon has been established, member vehicles are driven autonomously or semi-autonomously, and join/leave vehicles transition in and out of the platoon semi-autonomously [12]. While platooning offers considerable safety, economical, and energy benefits, the growing reliance on Dedicated Short Range Communication (DSRC) within CCAV platoons highlights potential vulnerabilities to cyberattacks [13]. Operations such as platoon formation, maintenance, merging, and splitting in CCAVs necessitate heightened situational awareness. Thus, safeguarding CCAVs from attacks that might disrupt their functions and jeopardise safety is crucial. Implementing strong cybersecurity protocols during the design and operation phases of CCAV platoons is essential to counteract these threats.

In response to security challenges, steps are being implemented to ensure that aspects such as Confidentiality, Integrity, Availability, and other critical security elements are integrated into the design and operation of CCAV systems. Despite these initiatives, research exploring the security threats and rigorous security measures for CCAVs ecosystem are in their infancy [6]. This research aims to conduct a comprehensive survey that examines the threat landscape of CCAVs utilising the platooning use case. This study makes a significant contribution to the field by providing a thorough analysis of a three-tier CCAV system, as outlined below:

- The paper presents an comprehensive survey of the threat landscape for CCAVs, compiling an extensive list of 132 threats from the literature, 64 documented real-life incidents (with timeline), and 22 specific threats related to platooning microservices.
- The study maps out a detailed attack taxonomy using identified threats, outlining 8 unique attack vectors for understanding 48 threats in CCAVs and platooning applications.
- The research identified and defines significant trust domains in a three-tier CCAV system, including 11 for CCAV, 12 for edge cloud, and 8 for core cloud.
- The paper emphasises the need for further research on dynamic, multifaceted optimal security strategies, including continuous security lifecycle management, adaptive threat modeling, and the implementation of Zero Trust principles.

To address the aim, this paper describes our research methodology in Section 2, and provides a comprehensive review of related works in Section 3. This is followed by an overview of CCAV technology and driving operations, which are specific to (but not limited to) platooning, in Section 4. Section 5 considers advances in CCAV security regulations and their implication on CCAV security design. The results of the survey of threats to the CCAV, Edge Cloud and Cloud systems are stated and analysed in Section 6 to identify impacted trust domains, with a particular focus on the platooning use case. These results are discussed in Section 7, through which an attack taxonomy was formulated and discussed. In Section 8, critical open challenges for securing CCAVs are described. Finally, the survey's findings on CCAV security threats are presented in Section 9, where we also provide recommendations for future research directions.

2. Methodology

To achieve the objectives of our research, we have undertaken a comprehensive survey and analysis of threats in the domain of CCAVs, drawing from both academic literature and real-world incident reports. This study begins by establishing a foundational understanding of CCAV technology, its various applications, and the inherent security

considerations. Our survey is primarily focussed on identifying and analysing prominent terms related to threats in the field of CCAVs, as recognised in established standards and extant literature. To collate relevant studies, we have employed a two-fold search strategy. Initially, we combined key terms such as "autonomous vehicle(s)", "connected vehicle(s)", or "driverless vehicle(s)" with terminologies such as "threat(s)" and "attack(s)", utilising Boolean operators such as "AND" and "OR" for a comprehensive search. Furthermore, we delved into specific threats associated with edge cloud and cloud-assisted CAV technologies. This involved searches for combinations of the aforementioned vehicle-related terms with concepts such as "edge cloud", "fog computing", "cloud-assisted", and "edge-cloud aided". Our literature search spanned across several pominent academic databases, including Scopus, ScienceDirect, Web of Science, IEEE, and Springer, with the scope of the search extending back to the year 2007.

In instances where these primary databases did not yield sufficient results, particularly due to a lack of citations and references, we supplemented our search with Google Scholar. This was, however, a secondary recourse to ensure the comprehensiveness of our survey. Additionally, to improve our understanding of current threats and to incorporate practical perspectives, we also referred to credible websites and news articles. The data sourced through this meticulous process has been carefully analysed to provide an insightful survey on the threats facing CCAV technology. By integrating academic findings with real-world threats, our study aims to present a well-rounded view of the security landscape for CCAVs. Through this approach, we seek not only to identify existing threats but also to anticipate emerging challenges and propose proactive strategies for enhancing the security of CCAVs. Adhering to the outlined methodology, this study has meticulously compiled a list of threats from the aforementioned sources. It also establishes an analytical timeline and attack taxonomy, inspired by CAPEC-1000 [14], pinpointing urgent security challenges that require further research within the specified trust domains of CCAV systems.

3. Related Works

In this section, we compare our research with related works. There are several surveys [15–37] related to the cybersecurity of CCAVs. However, this study sets itself apart by thoroughly examining threats related to literature, real-world events, and platooning in a comprehensive manner.

Numerous studies have not adequately addressed threat analysis for both in-vehicle and external attack surfaces. As shown in Table 1, the threats to CCAVs were classified in [28,36] and V2V/V2I communications were classified in [15–27,29–33,35–37]. Its impacts are highlighted in [31,32,34,36,37]; however, none have mapped and illustrated the threats with the trust domains. Common attack vectors were only discussed in [31,32,37], although an in-depth analysis of the vectors with taxonomy is not discussed. In addition, CCAV security standards can subsequently be used to refer to the latest developments. As such, our research presented here addresses the objectives through a comprehensive analysis of the CCAV threat landscape.

Table 1. Table comparing this research with existing surveys in CCAV cybersecurity.

Surveys	CCAVs	Edge/Cloud	V2V/V2I Communication	Threat Analysis	Attack Taxonomy	Real-Life Incident Timeline	Standards	Platooning
[15]	✗	✗	✓	✗	✓	✗	✗	✗
[16]	✗	✗	✓	✗	✗	✗	✗	✗
[17]	✗	✗	✓	✗	✗	✗	✗	✗
[18]	✗	✗	✓	✗	✓	✗	✗	✗
[19]	✗	✗	✓	✗	✗	✗	✗	✗
[20]	✗	✗	✓	✗	✗	✗	✗	✗

Table 1. *Cont.*

Surveys	CCAVs	Edge/Cloud	V2V/V2I Communication	Threat Analysis	Attack Taxonomy	Real-Life Incident Timeline	Standards	Platooning
[21,22]	✗	✗	✓	✗	✓	✗	✗	✗
[23]	✗	✗	✓	✗	✗	✗	✗	✗
[24]	✗	✗	✓	✗	✗	✗	✗	✗
[25]	✗	✗	✓	✗	✓	✗	✗	✗
[26,27]	✗	✗	✓	✗	✗	✗	✗	✗
[28]	✓	✗	✗	✗	✗	✗	✗	✗
[29]	✗	✗	✓	✗	✓	✗	✗	✗
[30]	✗	✗	✓	✗	✓	✗	✗	✗
[31]	✗	✗	✓	✓	✓	✗	✗	✗
[32]	✗	✗	✓	✓	✓	✗	✗	✗
[33]	✗	✗	✓	✗	✓	✗	✗	✗
[34]	✗	✗	✗	✓	✓	✗	✗	✗
[35]	✗	✗	✓	✗	✗	✗	✗	✗
[36]	✓	✓	✓	✓	✓	✗	✗	✗
[37]	✗	✗	✓	✓	✓	✗	✓	✗
This Paper	✓	✓	✓	✓	✓	✓	✓	✓

Tick (✓) and cross (✗) symbols are used to denote the presence and absence of topics, respectively.

4. Advancements in Connected and Autonomous Vehicles

CCAV technologies and the driving operations which they perform may be vulnerable to attacks. This section delves into the evolution of Vehicular Ad-Hoc Networks (VANETs) and Intelligent Transportation Systems (ITS), highlighting their role in enhancing communication, safety, and efficiency in transportation. It discusses the security challenges within ITS and the international efforts towards standardisation, despite concerns about competitive edge and implementation complexities. The focus then shifts to CCAVs, outlining their development in terms of autonomy levels and operational capabilities, and emphasising the importance of cloud and edge-cloud computing in V2V and V2I communications. This leads to a discussion on key CCAV communication technologies such as DSRC, WAVE/IEEE 802.11p, and 4G/LTE, essential for effective connectivity and minimal latency in CCAV operations among growing applications such as platooning.

4.1. VANETS and Intelligent Transportation Systems

Early research aimed to improve mobility, with significant progress focussing on Vehicular ad hoc Networks (VANETs). A VANET is a variant of Mobile Ad-hoc Network (MANET). VANETs support vehicular applications by providing wireless communication among vehicles and infrastructure [38]. Subsequent efforts focussed on achieving enhanced connectivity and real-time intelligent traffic solutions, laying the groundwork for Intelligent Transportation Systems (ITS) and related technologies. ITS aim to increase passenger safety while also improving passenger comfort and driving conditions. As communication between vehicles and RSU infrastructures grows, numerous ITS projects have collaborated to successfully achieve the following:

- Enhanced data exchange and precise data processing, leading to improved traffic safety and efficiency, ultimately resulting in standardised transportation [39].
- Collaborative vehicular applications that are networked with information-rich infotainment services.

- Proactive notification of real-time vehicle dynamics (location, speed, braking, etc.) by broadcasting awareness messages including unsafe and urgent local conditions (accidents, potholes, etc.) [40].
- An ecosystem whereby vehicles synchronise local events with CCAVs to make advanced analytical decisions.

While the features of ITS have improved over time, security has remained an important area of concern requiring resolution. Consequently, international organisations have collaborated to develop a safe and secure platform for a shared ecosystem [41–44]. One notable advancement from these initiatives has been the ITS architecture shown in Figure 1. The COMeSafety organisation has been instrumental in bringing together diverse CAV and ITS initiatives, resulting in the consolidation, harmonisation, and standardisation of ITS systems across IEEE, ISO, ETSI, and CEN [2,45]. While the adoption of a consistent architecture offers numerous benefits, it has also faced criticism for the following reasons:

- Standardised architectures result in the loss of distinctive competitive advantages;
- A standardised framework creates a single point of dependency, where any flaw in a dependent system can impact all vehicles;
- Establishing a national architecture and ensuring system-wide assurance poses significant challenges.

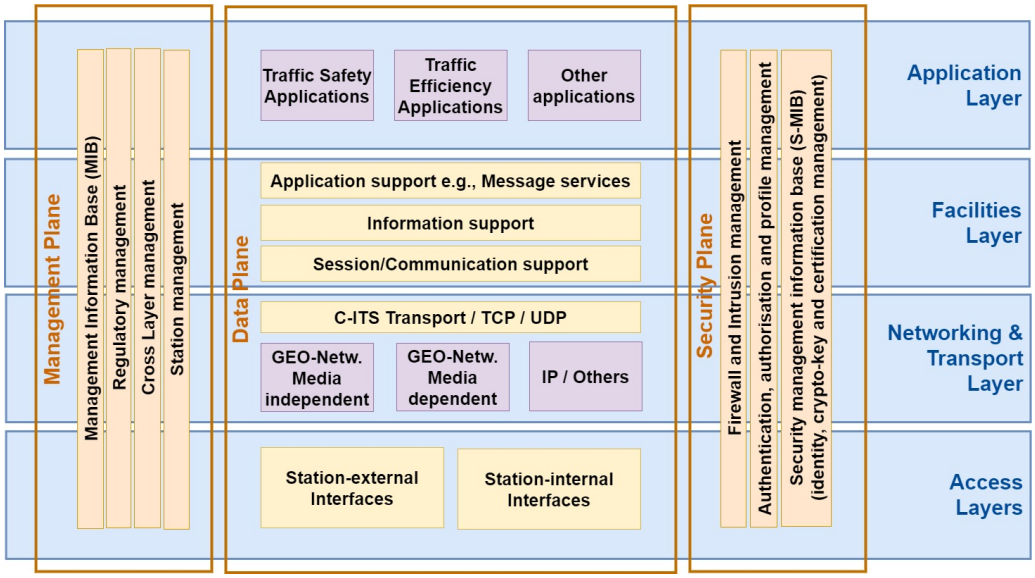

Figure 1. Functional view of ITS protocol architecture [45].

4.2. An Overview of CCAV

CCAVs are at an early stage of development. According to the literature and existing standards, CCAVs can be classified into six levels of functional autonomy based on the degree of human intervention [43,46]. Each level differs in its Operational Driver Domain (ODD), which defines the driving conditions that the vehicle it designed to handle. With an increasing vehicle autonomy level comes greater ODD and a more extensive capability in performable driving operations. Highly autonomous vehicles (Levels 4 and 5) additionally support fallbacks, which are procedures that come into effect if the ODD is exited. Further information on each level is provided in Table 2.

Table 2. Six driving automation levels [43].

SAE Level	Description
Level 0: No Automation	• Each driving operation is the responsibility of the driver. • ODD not applicable as the human driver controls the vehicle at all times.
Level 1: Driver Assistance	• Vehicle's use restricted to specific ODD. • Driver oversees driving tasks and monitors vehicle and environment. • Driver must intervene when vehicle exits ODD. • Equipped with systems for steering, acceleration, deceleration, and braking.
Level 2: Partial Automation	• System enables autonomous steering, acceleration, and deceleration. • Driver maintains responsibility for monitoring vehicle performance and functionality. • Object and event detection response operates within a specified ODD. • Despite advanced features, human supervision is essential for safety and effectiveness.
Level 3: Conditional Automation	• Object detection and advanced driving operations with minimal human intervention. • All operations are sustainable within a defined ODD. • Lacks fallback mechanisms if the vehicle exits the ODD. • ODD encompasses specific scenarios for system-managed driving tasks. • Driver required to override the system in emergencies.
Level 4: High Automation	• Vehicle is equipped with advanced technologies adapting to dynamic vehicle operations. • Sustainable driving within ODD, with fallback options if exiting ODD. • ODD covers diverse scenarios, yet restricted to certain areas or conditions. • System design permits driver intervention as needed.
Level 5: Full Automation	• Vehicle operates independently from human driver. All driving and fallback mechanisms performed autonomously. • ODD effectively limitless, covering all driving scenarios. • Vehicle capable of operating under all conditions autonomously.

The more advanced a self-driving vehicle's level of technology is, the better it can develop situational awareness and respond to its surroundings. Highly autonomous vehicles rely on real-time situational awareness in dynamic environments [47]. Modern sensors, processors, and computers are being studied for onboard and remote capability to enable seamless connection for collecting and analysing data relevant to the particular vehicular context for different applications [48]. Event Data Recorders (EDR), Global Navigation Satellite Systems (GNSS), RADAR, LIDAR, cameras, and memory storage are key hardware units for achieving enhanced situational awareness and intelligent mobility. Ethernet, USB, Bluetooth, FlexRay, Controlled Area Network (CAN), and Local Interconnect Network (LIN) are being further advanced for onboard communication [4]. Additionally, Dedicated Short Range Communication (DSRC) IEEE 802.11p is being developed for external communication [49]. CCAV communicate by V2V and/or V2I, cloud/edge cloud:

1. *Vehicle-to-Vehicle (V2V)*: Vehicles can communicate wirelessly with one another and preserve traffic safety by exchanging Basic Safety Messages (BSM) or Cooperative Awareness Messages (CAMs) to maintain a safe distance between vehicles, thus avoiding road accidents.
2. *Vehicle-to-Infrastructure (V2I)*: CCAVs and RSU are being developed to communicate with the external network (cloud, edge cloud, third-party, internet, etc.) by broadcasting or exchanging data related to road/traffic information and conditions in urban or highway scenarios. This is in addition to receiving the most up-to-date information about the local area. This enables vehicles to perform detailed analysis to make decisions based on the application. V2I-based applications are more bandwidth-intensive and require more CPU power than V2V-based applications [50].
3. *Cloud and Edge Cloud*: The literature has proposed two-tier architectures for CCAV applications, such as platooning [51]. However, they fail to discuss the stringent criteria of safety-critical CCAV applications due to the expected exponential growth in latency caused by communication and distributed computation. To address this, an interme-

diate layer called edge cloud was introduced to facilitate fog computing [52,53]. The edge cloud facilitates low-latency localised computation for CCAVs by establishing continuous communication with trusted infrastructures such as the core cloud and reliable third-party services while minimising communication latency. Consequently, a three-tier architecture is being considered for CCAVs, as depicted in Figure 2 for the platooning use case. This architecture comprises the core cloud, edge cloud, CCAVs, third-party services, and RSU infrastructures, as highlighted in various studies [53–56]. All such hardware and associated software would contribute towards the dynamics of a fully operable CCAV. Further information about the characteristics of CCAVs using their communication capabilities is detailed in Table 3.

Table 3. Characteristics of V2I and V2V communication, adapted from [15,17,19,26,29,39,50,57–59].

Characteristics of V2I Features	
Core cloud, edge cloud and RSU capabilities	Cloud infrastructures can execute remote functions to ease computation of resource-intensive tasks, providing eventful intelligence overall traffic, and vehicle management. The edge cloud could provide localised value-added services such as traffic updates, local events, and so on.
Heterogeneous size	Cloud services are envisioned to cater to individual and varying groups of CCAVs across several geographical regions.
Large scalable and unbounded network	Urban and rural areas, including highways, are to be connected across the nation. The network should be highly scalable and unbounded.
Dynamic network topology	CCAVs' mobility and change in the network can lead to wireless interference, challenging accurate and timely information for vehicular awareness.
Energy and real-time computation power	Connected infrastructures have powerful computational capabilities and should ensure high availability and reliability for CCAVs in order to provide real-time updates.
Communication	Regular communication of data packets will be through discrete and hybrid wireless communication channels, such as DSRC, WAVE, IEEE 802.11p, 5G, and 4G LTE.
Physical protection	Cloud, edge cloud, and RSUs would be installed with state-of-the-art technologies to support CCAVs. Physical protection of RSU is vital to prevent adversaries from tampering with any infrastructure components.
Predictability	The infrastructure units are needed to learn about the changing environment by collecting periodic updates. Through this data analysis, it is expected that additional information may be extracted to predict upcoming events, accidents, failures, traffic, etc.
Characteristics of V2V features	
Optimal processing power based on CCAV models	Different CCAVs have different capabilities which should be standardised to process messages through novel adaptive techniques.
Message broadcast	CCAV can broadcast periodic messages notifying the neighbouring vehicles of their whereabouts. This message would contain information about vehicle movement dynamics.

In this table, items in bold represent key categories within each CCAV characteristic area.

Cloud and edge cloud computing research has been primarily inspired by the research on Internet-of-Things (IoT) [51]. However, when it comes to CCAVs, which operate within three-tier cyber-physical systems, they differ from IoT devices in that they are mission-critical and time-sensitive. A notable advancement which uses a three-tier architecture is Cloud-Assisted Real-Time Methods for Autonomy (CARMA), a project financed by the EPSRC and Jaguar Land Rover [52,53]. Each component within this architecture possesses distinct capabilities. For further details on these capabilities, see Tables A6 and A7 in Appendix A. The core cloud, responsible for delivering computing power essential for optimizing mission planning and managing mobile infrastructures, security, databases,

maps, and third-party applications, also extends its services to the edge cloud. The edge-cloud facilitates low-latency localised computation for CCAVs by establishing continuous communication with trusted infrastructures such as the core cloud and third-party services. The edge cloud performs off-board vehicular computation, analyses regional maps, and executes security algorithms such as the authentication of CAMs.

All such operations require reliable and robust software. Data fusion, categorisation, object identification, warnings, localisation, and detection are utilised to separate and construct usable vehicular contexts through data analysis. CCAVs (at SAE level 5) serve as an end node for monitoring, sensing, and constructing environmental and traffic data that may be utilised for prediction and better manoeuvrability. This unique capacity of CCAVs to perceive and create data needs fast processing and decision-making algorithms, for which edge cloud and core cloud can provide aid [15,28,46].

4.3. Key Communication Developments for CCAVs

The operation of CCAVs necessitates a comprehensive understanding of their surroundings, which is managed by the establishment and enhancement of situational awareness. Two essential V2V communication technologies for providing situational awareness are Wireless Access for Vehicular Environments (WAVE)/IEEE 802.11p and DSRC, respectively, [17]. To increase awareness, messages such as CAM or BSM and Decentralised Environmental Notification Message (DENM) are expected to be transmitted through V2V communication. Message standards are also being revised and updated. Additional technologies, such as 4G/LTE and 5G, are being investigated to provide V2I connectivity to cloud environments, enabling seamless communication and computing capabilities for CCAVs with minimal latency.

In the United States and Europe, DSRC has two variations in channel allocations and operates over 10 MHz. The Federal Communication Commission (FCC) in the US has allocated seven bandwidth channels, whereas it has been allocated five bandwidth channels in Europe. Ch 178 and 180 serve as Control Channels (CCH) in the United States and Europe, respectively, and the remaining channels are termed as Service Channels (SCH) [15]. The IEEE 802.11p protocol has been introduced to the IEEE 802.11 protocol family to facilitate DSRC-based vehicle networks. The physical and medium access layers are further detailed in IEEE 802.11p-2010 [60]. The physical layer of IEEE 802.11p is based on IEEE 802.11a, whereas the Quality of Service (QoS) layer is based on IEEE 802.11e.

4.4. CCAV Applications

The three-tier design of CCAV offers adequate bandwidth and processing capabilities to enable the development of useful CCAV applications. These applications are classified into two broad categories: onboard and off-board connectivity-based services [17]. Automatic collision warning, roadside assistance, diagnostic information, remote door handling, hands-free speech, and location-based services are some functions that are included in the on-board applications. For a detailed list of the applications that contribute to the broader ITS capabilities, refer to Table A1 in Appendix A. These applications may communicate and coordinate with third-party services using external communication technologies to exchange application-specific data. GM Onstar is an example of an automobile that has been developed with these functions [28,61–63]. On the other hand, V2X-based vehicles such as Tesla have detailed functions that communicate with their servers remotely. These are being developed further to include [62]:

1. *Information Services*: Fault prediction and response, data collection and generation, data dissemination and distribution, efficiency improvement, and convenience services;
2. *Safety Services*: Collision avoidance, hazard reporting, and driver profile and monitoring;
3. *Individual and Group Motion Control*: Connected and autonomous driving and vehicular platooning.

CCAV applications have been categorised broadly into Infotainment and Comfort, Traffic Management, Road Safety, and Autonomous Driving [17,26]. The US Department

of Transportation [2] has proposed a similar set of functions, which this research has also considered. The objectives of these applications are:

- To support drivers with vehicles classified under specific SAE automation levels, ranging from Level 2 (Partial Automation) to Level 5 (Full Automation), by providing proactive collision warning signals to drivers, passengers, and pedestrians in order to reduce traffic accidents;
- To deliver real-time alerts to assist in traffic management by offering the most up-to-date road conditions and navigational services, as well as planned detours in the event of an accident;
- To provide value-added services, such as keeping track of a driver's profile and a vehicle's profile personalised entertainment options.

Platooning

As highlighted in the list of CCAV applications (Table A1, Appendix A), the platooning application is becoming increasingly popular, a trend underlined by its various advantages [64]. Currently, CCAV platoons are researched with three key topologies: centralised, decentralised, and hybrid. In a centralised topology, the lead vehicle communicates with all vehicles in the platoon, but member vehicles do not communicate with each other [65]. The lead receives and processes information from the member vehicles and then transmits commands to each vehicle. In a decentralised topology, each vehicle communicates only with the vehicle directly behind it. In a hybrid topology, there are four main combinations of centralised and decentralised topologies, which are: fully centralised, fully decentralised, centralised and decentralised, cluster-based or hierarchical [10]. CCAV follow a hybrid approach. Here, platooning relies on cloud infrastructure, Figure 2, and its operation can be decomposed into the microservices it performs. These microservices are [64]:

- *Formation*: This functionality enables multiple CCAVs to come together and form a cohesive unit, typically through communication and coordination with other vehicles and traffic management systems;
- *Management*: This functionality encompasses tasks such as maintaining safe inter-vehicle distance, adjusting speed to match traffic conditions, and ensuring the safe and efficient operation of all vehicles in the platoon;
- *Joining*: This functionality allows integrating additional CCAVs into an existing platoon, typically through communication and coordination with the platoon leader and other vehicles;
- *Leaving*: This functionality allows for the safe exit of a CCAV from a platoon, typically through communication and coordination with the platoon leader and other vehicles;
- *Merging*: This functionality enables the consolidation of multiple platoons into a larger unit, typically through communication and coordination with the platoon leaders and other vehicles;
- *Splitting*: This functionality allows dividing a platoon into smaller units, typically through communication and coordination with the platoon leader and other vehicles;
- *Ending*: This functionality enables the safe dissolution of a platoon, typically through communication and coordination with the platoon leader and other vehicles;
- *Leader Change*: This functionality allows transferring leadership responsibility within a platoon, typically through communication and coordination with the current platoon leader and other vehicles.

Given that platooning microservices are vulnerable to attacks (Table A2), due to its reliance on external connectivity and developed situational awareness as described in Section 4.2, it becomes crucial to explore the threat landscape of CCAV within the context of the platooning application.

The layers in ITS architecture, as demonstrated in Figure 1, is currently under research for deployment with platooning scenarios in both SAE Level 4 and Level 5 applications

(Table 2). Incorporating systems and functionalities into a three-tier architecture system, as depicted in Figure 2, for platooning microservices, reveals significant intersections with various other CCAV applications. These encompass parking, adaptive cruise control, braking, merging, and lane changing, as outlined in Table A1. Consequently, conducting a comprehensive analysis of the threat landscape for vehicles operating in a platoon is imperative to gain a systematic understanding of the core functionalities of CCAV systems. This exploration is particularly significant due to its potential impact on safety in the event of an accident.

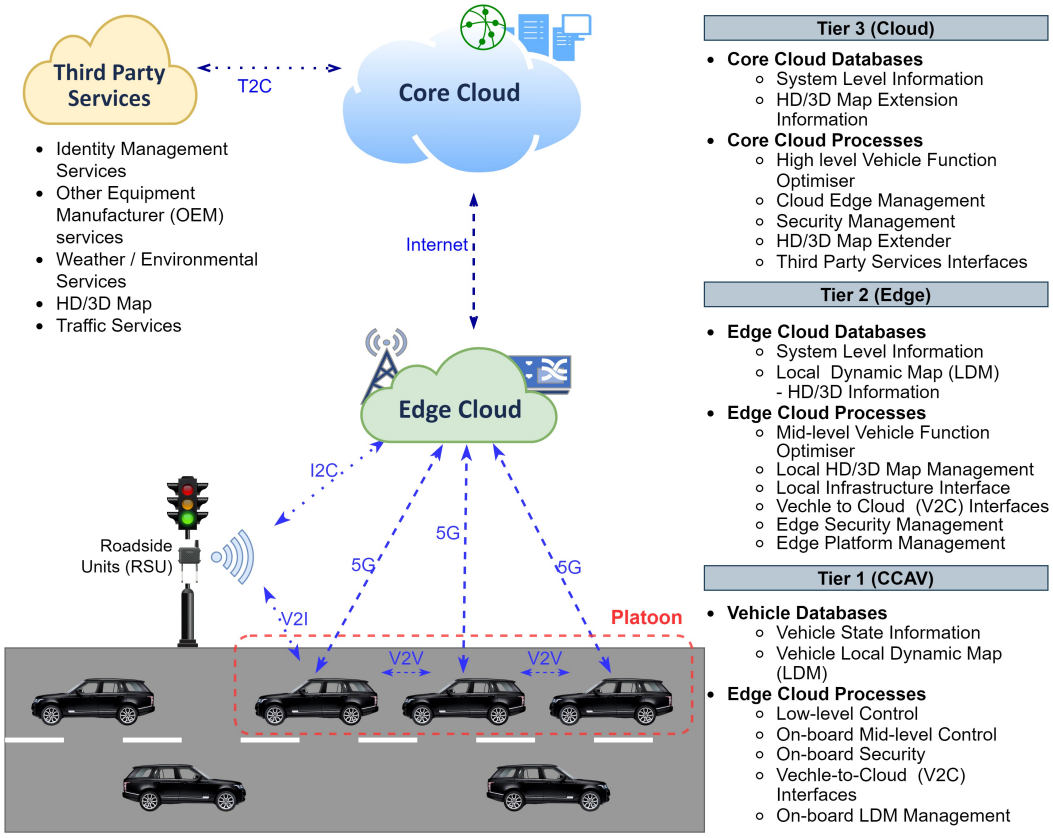

Figure 2. Three-tier CCAV high-level view (with platoon).

5. Advancements in CCAV Security

This section introduces the fundamental concepts of security in cyber-physical systems, particularly focussing on CCAVs. It covers key security aspects such as confidentiality, integrity, and availability, essential for protecting CCAVs against cyber threats. The discussion sets the groundwork for understanding the complexities and challenges in implementing robust security measures in this evolving technological domain.

5.1. Fundamentals of CCAV Security

Security in an cyber-physical systems is practised based on the division and the protection required for specific assets or activities. It encompasses various aspects, such as risk management, IT security, physical security, identity and access control, personnel security, and procedural security [66]. A secure entity, as defined by [67], is an environment that ensures safety and predictability, allowing uninterrupted operation for systems, individuals, or organisations. The following requirements define security in the context of CCAVs [17,50,68–70]:

1. *Confidentiality*: CCAV systems should be capable of encrypting and decrypting data on a need-to-know basis. Data storage that is not confidential may result in data exposure, leading to potential data breaches and passive attacks such as eavesdropping.

2. *Integrity*: Transmitted data packets will update the edge cloud and cloud. These include CAM, DENM, and value-added services. Data integrity checks protect against manipulation, alteration, or erasure. Validation tests using hash algorithms ensure data integrity during transmission and storage. Data integrity attacks include manipulation, fake data generation, and impersonation.
3. *Availability*: To ensure uninterrupted access to safety-critical applications, the edge cloud and cloud systems must be resilient against hardware or software failures, power outages, and cyberattacks. Availability is essential. Denial-of-Service (DoS) attacks, jamming, greedy behaviour, blackholes, grey-holes, sinkholes, wormholes, broadcast manipulation, malware, and spam are all threats to the availability of CCAVs.
4. *Auditability, Traceability, Accountability, Non-Repudiation, and Revocability*: Malicious messages can impact CCAVs, causing errors, incidents, and even accidents. Techniques for detecting altered data post-processing should exist for auditability. For example, CCAVs should record each message shared by the edge cloud using unique message IDs in order to create auditability and accountability. As a result, anomalies are monitored by the edge cloud's Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS), and hostile nodes are identified and reported to the Trusted Authority (TA). This approach enables the withdrawal of security permissions for suspicious or malicious nodes and any other erroneous entities.
5. *Authenticity and Verifiability*: CCAVs must develop confidence in the edge cloud and neighbouring vehicles. As a result, verifying the authenticity of messages is important for time-sensitive and safety-critical applications. Verifying messages for real-time situational awareness requires optimally efficient deterministic schemes. Tunnelling, node impersonation, GPS spoofing, and Sybil attacks are some techniques that may jeopardise the validity of messages (CAM/DENM/etc.).
6. *Privacy*: Personally Identifiable Information (PII) of the vehicle owners, drivers, and passengers should not be disclosed by CCAV systems. For example, organisations may wish to share CCAV IDs with third-party organisations. Users should be given a choice to control their respective data. Long-term anonymity and differential privacy are some methods that are being researched to protect the CCAV system.

5.2. Key Developments for CCAV Security

There is a collection of existing standards that are relevant to CCAV security from the United States, Europe, China, Republic of Korea, and Japan [32,40–43,71]. Each nation is continuing to develop relevant standards in accordance with scientific discoveries and to meet the socioeconomic market needs in their respective countries. Consequently, different countries design vareity of software and hardware to conform to their own CCAV specifications, leading to variations in their communication and security protocols. This has created a worldwide challenge in which vehicles are sold and used in multiple countries, with each vehicle manufacturer required to adhere to local requirements. This practice makes development harder and can lead to variations in how security is handled and set up. This discontinuous development could result in CCAVS being unable to interact with other nodes in an ecosystem because of the security vulnerability introduced into other safety-critical systems. Collaboration among nations was recognised as being critical to overcoming this issue.

5.2.1. Harmonization Task Groups

To address the issue of differing version and inconsistent standards, the EU–US Harmonization Task Groups (HTG) were established. HTG comprises two groups: HTG1 focuses on security standards, while HTG3 handles communication standards. They aim to agree among manufacturers on the secure interoperability of cooperative vehicular systems [44]. These organisations have documented their findings, identifying commonalities and highlighting technical issues, such as the Basic Service Set (BSS) in wireless communication across ISO, ETSI, IEEE, CEN, and SAE standards. HTG1 acknowledges

that IEEE security standards are reasonably well harmonised but emphasises the need to address security challenges, including regulatory and policy definitions, for the public benefit. Meanwhile, HTG3 acknowledges differences in communication protocols between EU and US standards.

ETSI has produced several standards for privacy and security in ITS. These include (i) ETSI TR 102 893—Threat, Vulnerability and Risk Analysis (TVRA), (ii) ETSI TS 102 867— Stage 3 mapping for IEEE 1609.2, (iii) ETSI TS 102 943—Confidentiality Services, (iv) ETSI TS 102 941—Trust and Privacy Management (v) ETSI TS 102 942—Access Control, (vi) ETSI TS 102 940—ITS communication security architecture and security management, and (vii) ETSI TS 103 097—Security header and certificate formats.

5.2.2. ISO 26262

ISO26262 [42] standard was first published in 2018 and has been revised since. It is intended for use with safety-related systems, including one or more Electrical and/or Electronic (E/E) components, and is integrated into the newest vehicles. ISO 26262 helps design a company-specific development framework in which certain criteria are technical in nature while others are process-related and demonstrate an organisation's functional safety capabilities. The framework refers to systems that may be classified as connected vehicles; nevertheless, the degree of autonomy is determined by the manufacturer's most recent output. Additionally, the standard discusses the following:

- Modifications to existing systems and their components that have been deployed for production prior to the latest standard by customising the safety lifecycle for each modification;
- Integration of older systems by modifying the safety lifecycle;
- Tackles potential dangers resulting from the defective activities of safety-related E/E systems, including their interaction.

5.2.3. ISO/SAE 21434

ISO/SAE 21434 [41] was updated most recently in 2021. It aims to integrate cybersecurity into the design of E/E systems for vehicles, addressing the issues related to sophisticated networked technologies and its growth in the number of attacks with resulting tactics and techniques. It covers the need to establish consistent cybersecurity engineering goals, criteria, and methods across the automotive supply chain. As a result, organisations can:

- Develop policies for cybersecurity;
- Manage associated security risks;
- Foster developing security practices and culture within the organisation.

5.2.4. SAE J3061

The SAE J3061 [43] standard was first published in 2016 but updated in 2021. It establishes a set of high-level cybersecurity concepts relevant to cyber-physical vehicular systems, including recommendations for the safety and security of the system. Unlike the prior standards, SAE J3061 distinguishes itself by integrating guidance to solve security concerns in the automotive supply chain and production processes by considering safety challenges. This might be considered as a strategy for integrating security-by-design throughout the product's lifespan. The standard aims to address the following:

- Integrating cybersecurity into cyber-physical vehicular systems across the development, manufacturing, operation, maintenance, and decommissioning processes;
- Describes some current tools and methodologies for creating, verifying, and validating CAV systems;
- Introducing key cybersecurity principles for automotive systems and establishing the framework for future vehicle security standards.

On consideration of these standards and despite global initiatives to coordinate and integrate vehicle security solutions, there have been few attempts to address security concerns specific to the dynamic nature of connected vehicles. Security is vital to mitigate disruption caused by threats such as fraudulent communications, impacting both cars and infrastructure systems. Trust, efficiency, and resilience are significant challenges in the standardisation process. Moreover, privacy emerges as a critical issue, as anonymous message transmission for non-traceability and user monitoring adds complexity and necessitates accountability and non-repudiation measures. In the subsequent section, we aim to mitigate these drawbacks by comprehensively analysing the threat landscape. This analysis involves a thorough examination of the existing literature, investigating real-life incidents, and scrutinising the platooning use case to gain insights into the trust domains and prevalent attack mechanisms.

6. Threat Analysis

Understanding the various threats faced by CCAV systems is crucial for understanding the attack mechanisms. To do so, this study identifies security vulnerabilities in the literature, real-life, and platooning cases to define the impacted trust domains. Furthermore, their implications on the trust domains and platooning microservices are explored.

6.1. General Threats

This section is classified into two subsections: threats from the literature and threats from real-life incidents. This categorisation is important because notable overlap exists between real-life incidents and those identified in the literature. Such overlaps occur because the literature often anticipates or is based on emerging patterns of threats observed in real-world scenarios. For instance, threats from sources such as "Jeep and Chrysler can be remotely hacked, 1.4 million cars and truck recalled", frequently discussed in scholarly articles, have also been discussed in real-life incidents [72]. This overlap is crucial as it validates the predictions and models presented in the literature [5], offering a more comprehensive understanding of potential threats. However, certain threats may be unique to each domain. Literature can delve into hypothetical scenarios or emerging technologies not yet encountered in the real world, exploring threats that are theoretical or forward-looking. Conversely, real-life incidents might reveal unforeseen vulnerabilities or contextual factors that were not previously considered or apparent in academic studies. This distinction underlines the importance of a multi-faceted approach to threat assessment in CCAVs.

This classification is also important to highlight that the media's coverage of threats significantly impacts the automotive industry. Academic or theoretical threats, when reported, can influence public perception and industry reputation, even if they have yet to occur in reality. In contrast, real-life incidents, when highlighted, provide concrete evidence of threats, leading to immediate public concern and potentially urgent regulatory and industry responses. Moreover, real-world incidents have a more direct and substantial influence on public perception compared to theoretical threats. Tangible examples of CCAV failures or security breaches can swiftly sway public opinion and prompt regulatory action. While literature-based threats are crucial for strategic planning, they may not provoke the same level of immediate public concern due to their abstract nature, underlining the need for the industry to address both types of threats effectively [73,74]. Therefore, this section first dives deeper into threats from the literature and then explores the threats reported in the public.

6.1.1. Threats from the Literature

Our review of threats from the literature found that the number of threats identified for the CCAV tier (76) exceeded those identified for the Edge/Cloud tier by 26%. This discrepancy suggests a heightened propensity for vulnerabilities within CCAVs compared to the infrastructure supporting them. These threats encompass various attack mechanisms that

an adversary could employ to gain unauthorised access, control, or even disable the system. Consequently, these vulnerabilities could lead to system malfunctions or pose significant risks to human safety. Our complete results, which describe threats to platooning, CCAV, edge cloud, and cloud are contained within the Appendix A in Tables A2, A6, A7 and A8, respectively.

Further analysis of these security threats revealed recurring instances of compromised system domains, each targeted through different attack vectors. Due to the interconnectedness of these domains and the potential for overflow of these impacts on the connected domains, we have categorised these threats according to the impacted trust domains. Based on our analysis, we identified 11 trust domains in the CCAV tier, 12 in the edge cloud, and 8 in the core cloud tier, all of which possess vulnerabilities (see Table 4). Wireless communication, energy systems, and physical input/output emerged as common trust domains across the CCAV, edge cloud, and cloud tiers. However, specific trust domains exclusive to CCAVs include the infotainment system and the human-machine interface (HMI). For a detailed description of the identified trust domains, refer to Appendix A Tables A3–A5.

Table 4. Identified trust domains on CCAV, edge cloud, and core cloud tier.

	Trust Domains		
Sr. No.	**CCAV (V-TD)**	**Edge Cloud (E-TD)**	**Cloud (C-TD)**
1	Wireless Communications	Wireless Communications	Wireless Communications
2	Infotainment	Microservices	Data Analysis
3	Data Storage	API	Microservices
4	Vehicle Sensors	Physical I/O	API
5	Physical Input/Output	Process	Data Analysis & Data Storage
6	Monitoring	Data Storage	Monitoring & logging
7	HMI	Energy Systems	Physical I/O
8	Energy System	Actuators	Energy System
9	Actuators	Monitoring	
10	Data analysis	Sensors	
11	Devices and peripherals	Devices	
12		Roadside Infrastructure	

6.1.2. Threats from Real-Life Incidents

Traditionally, vehicles were developed with an emphasis on speed and safety over security, leaving them vulnerable to various attacks. Exploiting weaknesses in on-board entities and wireless communication channels, such as cellular connections, Bluetooth, and physical endpoints such as Onboard Diagnostic Unit (OBU) ports, have proven to be effective [4,5,75]. To enhance understanding of actual vehicle attacks, Figures 3 and 4 and Table A8 provide a comprehensive overview of 64 publicly disclosed incidents from 2011 until the end of 2022. The table includes the Real-Life Incident Code (RL-IC), trust domain, date, incident title, and the threat description.

There have been a number of notable real-world attacks that have compromised the safety and security of vehicles. In 2011, Checkoway et al. announced the first remote hack of a vehicle, gaining control of a Chevy Malibu (2011) [75,76]. They gained access to low-speed and high-speed Control Area Network (CAN) through the vehicle's radio and vehicle's telematics unit by exploiting a vulnerability in the Bluetooth stack from a synced phone. This enabled communication with the actuators and the attacker could rapidly apply the brakes.

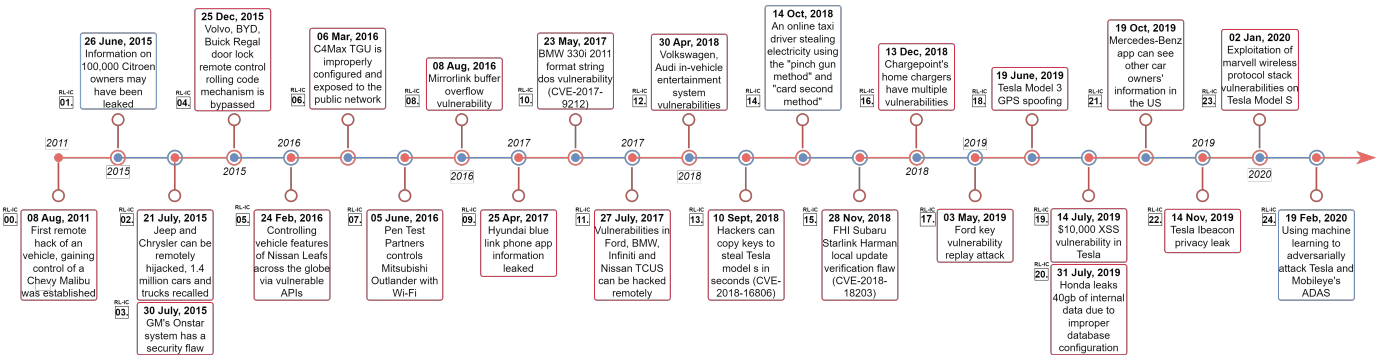

Figure 3. Real-life incidents—Timeline 1.

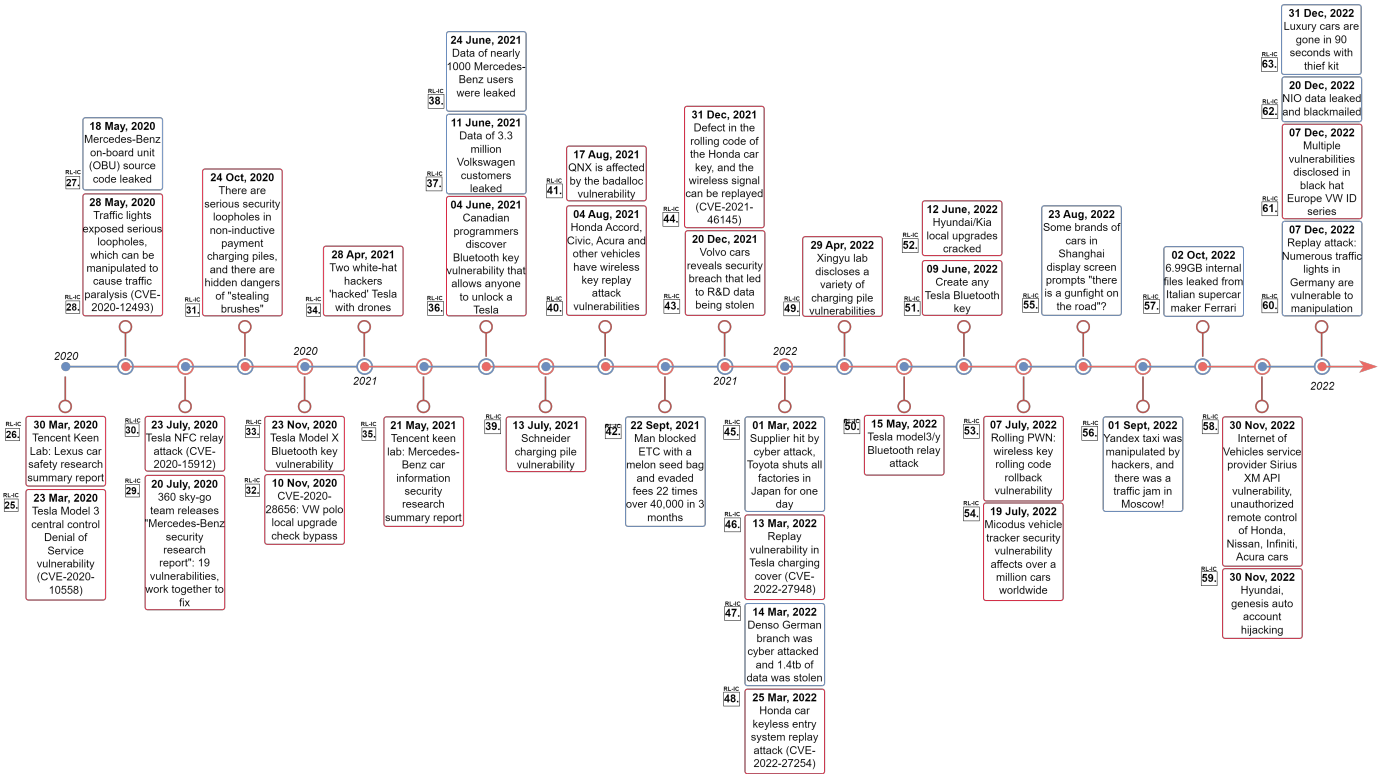

Figure 4. Real-life incidents—Timeline 2.

In 2015, Miller and Vallesek's [4] investigation of vehicular attacks proved seminal. since it was a remote exploitation of a system threat in the Jeep Cherokee. This led to seizing control of the steering. This quickly captured the attention of the media, because the attack could be spread to 1.4 million vehicles. This raised concerns and quickly highlighted the rising risk of on-board and remote attacks. The following year, Tencent's Keen Security Lab hacked a Tesla Model S remotely [77]. They took advantage of an obsolete web browser in the Central Instrument Display (CID). The attack may be carried out by deceiving a victim into visiting a malicious website. If the car had previously connected to a well known Wi-Fi network, an adversary may get access to it and reprogram the gateway device using a CID vulnerability. This enabled them to communicate with the vehicle's brakes through CAN signals. Following this, Tesla eventually added code signing to the gateway to prevent reprogramming [77].

In 2018, Tencent Keen Security Lab discovered 14 vulnerabilities in the Infotainment System, Telematics Control Unit (TCU), and Central Gateway Module components of several BMW models (BMW i3, BMW X1, BMW 525, and BMW 730) after performing an in-depth security analysis. All software flaws were addressed by online reconfiguration and offline firmware updates (not Over-The-Air (OTA) update) [78]. Furthermore, recently,

in 2022, Tencent Keen Lab pen-tested Mercedes Benz's infotainment system (primary infotainment ECU) and TCU to find security flaws. They physically obtained access and then leveraged remote access to the head unit of the vehicle. This allowed the researchers to adjust the colour of the interior lights, show photos on the infotainment screen, and execute other activities [79].

Similarly, there have been other threats that were identified and declared in real life and the literature. Building on the understanding from the identified trust domains, and the nature of these threats from the literature, the impact of these 64 RL-IC was further analysed for their impact on the three-tier CCAV system. In real-life scenarios, a significant elevation of threats associated with CCAVs (86) has been observed versus the Edge/Cloud tier (32) (Table 5). This tangible disparity signals a greater number of security threats directed at the CCAVs themselves, which might encompass issues of vulnerabilities that can be physically accessed, comprising cyber-threats targeting the vehicle software or communication.

Table 5. Total impact count of identified threats based on the literature, real-life, and platooning cases.

Threats	CCAV	Edge/Cloud
Literature	76	56
Real Life	86	32
Platooning	86	94

6.2. Platooning Threats

As previously stated in Section Platooning, the CCAV platooning application is garnering much interest due to its associated economic, logistical, and safety benefits. However, vehicles within a platoon are vulnerable to the exploitation of threats by adversaries. The literature covering the platooning security threats, including those affecting trucks, revealed 22 security threats impacting microservices [65,80]. These threats are described in detail in Table A2, which further explains the impact of such threats on the eight microservices of platooning for the three-tier CCAV system.

The analysis of CCAV platooning microservices reveals the complex security landscape of the system. Several threats pose risks to the different microservices involved. Covert Channel and Black Hole attacks affect all microservices, compromising communication, integrity, and overall functionality. Forming, Managing, Joining, Leaving, Merging, Splitting, Ending, and Changing Leader microservices are the most affected, being susceptible to a wide range of threats including Jamming Attacks, Malware or Ransomware, and Impersonation Attacks. Eavesdropping, Data Collection and Information Theft, and Location Disclosure do not specifically target any microservices, highlighting the need to address overall data security and privacy concerns.

Upon analysing the platooning threats and considering insights from the literature and real life, a concerning amount of platooning security threats are identified for both CCAVs (86) and Edge/Cloud tiers (94) (Table 5). The intricate nature of platooning scenarios, such as the reliance on inter-vehicle communication and centralised control strategies, likely contributes to this elevated threat level.

The threat landscape of CCAV using the platooning use case was analysed from a high-level viewpoint. This research analysed threats theoretically from the Literature (L), Real-Life (R), and Platooning (P) cases, with a concentration on inter-vehicle (V2X) and intra-vehicle threats (onboard).

Although the findings give us an overview of all the identified threats, they have not been categorised based on attack mechanisms. A taxonomy inspired by CAPEC-1000 was mapped in the following section. This helps us in understanding further with validity of the overlaps of L, R, and P threats. It is also important to note that the identified threats and approaches may offer valuable insights into other CCAV functionalities and applications, underscoring the broader applicability of our findings in the CCAV landscape.

6.3. Impacted Trust Domains

The number of times each Threat–Trust Domain pair occurs in the edge cloud, cloud, and CCAV provides valuable insights into the distribution and frequency of different threats across various trust domains. The bar graphs shown in Figures 5 and 6 provide a clear and concise overview of these threats and their distribution across different trust domains in L, R, and P systems. As a result, the following observations were made:

- The trust domain "V-TD1" (Wireless Communications) has the highest number of platooning threats, followed by "V-TD11" (Devices and Peripherals) and "V-TD10" (Data Analysis). In the edge cloud and cloud, the trust domain "E-TD1, C-TD1" (Edge Communication) has the highest number of threats, followed by "E-TD12" (Roadside Infrastructures) and "E-TD5, C-TD2" (Edge Processing and Data Analysis). This suggests that these areas might be the most vulnerable in the context of platooning.
- The trust domain "V-TD9" (Actuators) has the highest number of real-life threats followed by "V-TD2, V-TD7" (Infotainment, Human Machine Interface (HMI)). In the edge cloud and cloud, the trust domain "E-TD6, C-TD5" (Data Storage) has the highest number of threats, followed by "E-TD12" (Roadside Infrastructures) and "E-TD3, C-TD4" (Application Program Interface (API)). This indicates that these domains have been exploited in real-world scenarios, and thus, require significant attention.
- The trust domain "V-TD4" (Vehicle Sensors) has the highest number of literature threats. This is because vehicle sensors are a critical component of autonomous vehicles and any compromise in their functioning can lead to subsequent inferences and severe consequences.
- Some trust domains, such as the Physical Input/Output, Monitoring, and Logging trust domains, have relatively fewer threats across all categories. However, this does not necessarily mean that they are less important. The impact of a threat also depends on the severity of its consequences; however, they may have a low likelihood.

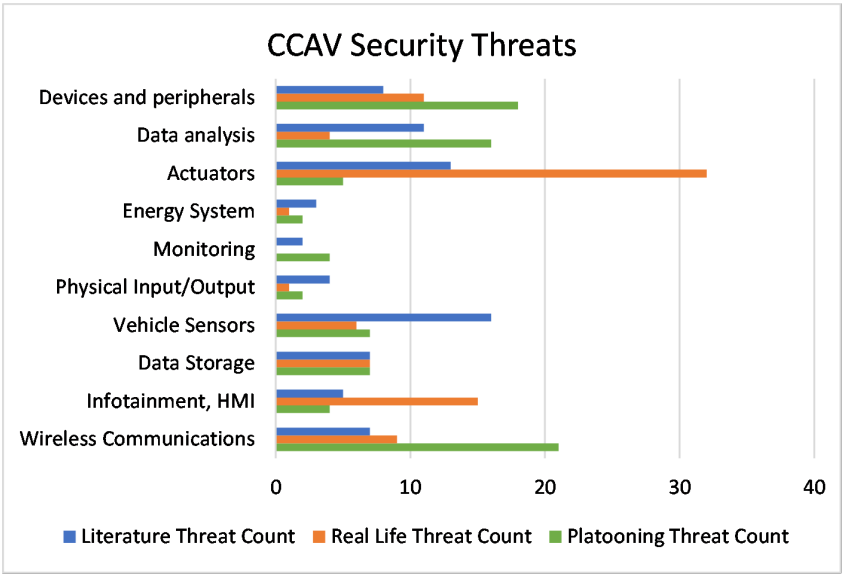

Figure 5. CCAV security threats—literature review, real life, and platooning threats analysis.

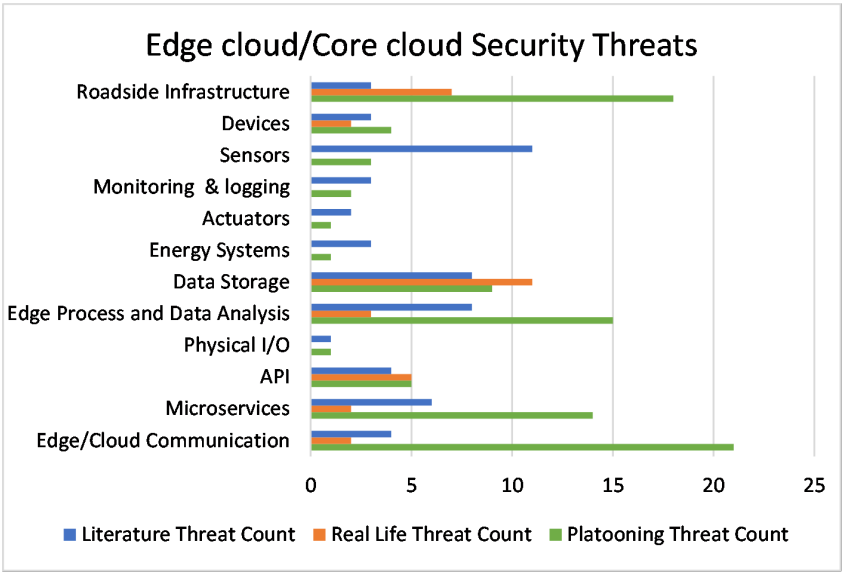

Figure 6. Edge cloud/core cloud security threats—literature review, real life, and platooning threats analysis.

7. Discussion

There is a considerable variation in the number of threats across different trust domains and categories. This underscores the need for a comprehensive and tailored approach to threat management in CCAVs and platooning. This analysis can guide the development of effective security strategies and measures to mitigate these threats. Some key observations and discussions that can be formed from the L, R, and P threats in Figures 5 and 6. Our complete results, which describe threats to platooning, CCAV, edge cloud, and cloud, are contained within the Appendix A, in Tables A2, A6, A7, and A8, respectively. From this, the following can be obeserved:

- It is seen that the number of threats affecting each trust domain gives us an idea of which trust domains present a high concentration of threats. For example, in the CCAV, trust domains "V-TD1", "V-TD9", "V-TD10", and "V-TD11" are affected by most identified threats in L, R, and P. In the edge cloud, the trust domains "E-TD1", "E-TD2", "E-TD5", "E-TD6", and "E-TD12" are affected by most identified threats in L, R, and P. This suggests that these trust domains may be more vulnerable and may require additional security measures discussed in Section 8. In addition, from analysing platooning, it is also observed that the 'Black Hole' threat appears across all trust domains in both the edge cloud and CCAV, which indicates it is a threat that can have severe consequences if an adversary can exploit it.
- The comparison between the edge cloud and CCAV shows that the distribution of threats across trust domains is different. This suggests that the security measures and strategies may need to be tailored differently for the edge cloud and CCAV.
- The frequency of threats across trust domains can help in prioritising security measures. Trust domains that are associated with a higher number of threats or with more severe threats might need to be prioritised.
- The bar graphs can also be used for security planning. By knowing which trust domains are most affected by threats, security teams can plan and allocate resources more effectively. For example, more resources might need to be allocated to protect trust domains that are affected by a higher number of threats. This information can be used to develop targeted security measures for each trust domain based on the threats they are most likely to face.

Therefore, we have identified plausible and vulnerable trust domains; however, trust domains are the final area of impact. From these impacted trust domains, it would be beneficial to derive attack mechanisms. From our analysis and discussion, we have identified

the following attack mechanisms described in Section 7, which lay the foundation for our attack taxonomy. Further details on the attack mechanisms can be found in their respective threat descriptions in Tables A6 and A7 in Appendix A.

From our results, we created an attack taxonomy by mapping L, R, and P. The attack taxonomy, as illustrated in Figure 7, is a systematic categorisation of the potential threats faced by CCAV systems. The threats have been classified according to the widely recognised CAPEC-1000 system, which includes the following categories: "Deceptive Engagement", "Abuse of Functionality", "Manipulation of System Resources", "Injection of Unexpected Data", "Subversion of Access Controls", "Data Collection and Analysis", "Employment of Probabilistic Techniques", and "Manipulation of Timing and State".

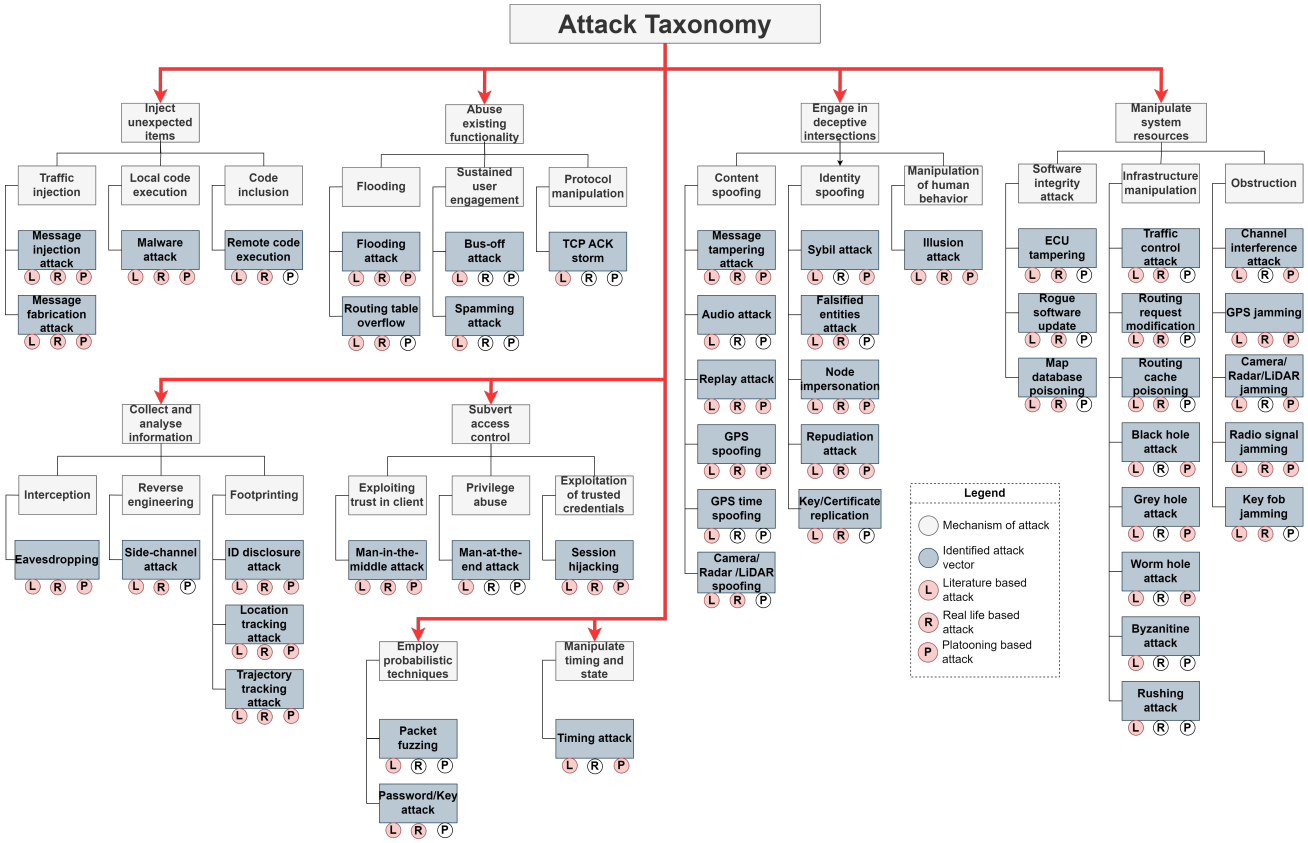

Figure 7. Mapping of documented threats, vulnerabilities and attacks from the literature, real-world scenarios, and platooning use-cases onto a modified attack taxonomy based on CAPEC-1000 attack mechanisms [81].

This taxonomy provides a comprehensive and concise summary of the identified threats, including their mechanisms, vectors, and distribution. This serves as a valuable tool for security professionals in the analysis of attack paths and the identification of critical security weaknesses. The high-level representation of threats in the taxonomy enables manufacturers to prioritise mitigation efforts and enhance the overall security of CCAVs and the platooning application.

The comprehensive analysis of threats relevant to CCAVs, particularly in the context of platooning, reveals a total of 250 threats derived from both literature and real-life incidents. Out of these, 180 are applicable to platooning. The graph accompanying this analysis (Figure 8) illustrates that the threats identified in this paper are extensive, with a count of 48 from the taxonomy. These threats have been meticulously detailed and demonstrate overlap across various trust domains, emphasising the complexity of the security landscape in the CCAVs, edge cloud, and cloud, as shown in Appendix A. Notably, the summarised

taxonomy, which distills these threats, maps them effectively across the literature *L*, real-life incidents *R*, and platooning scenarios *P*.

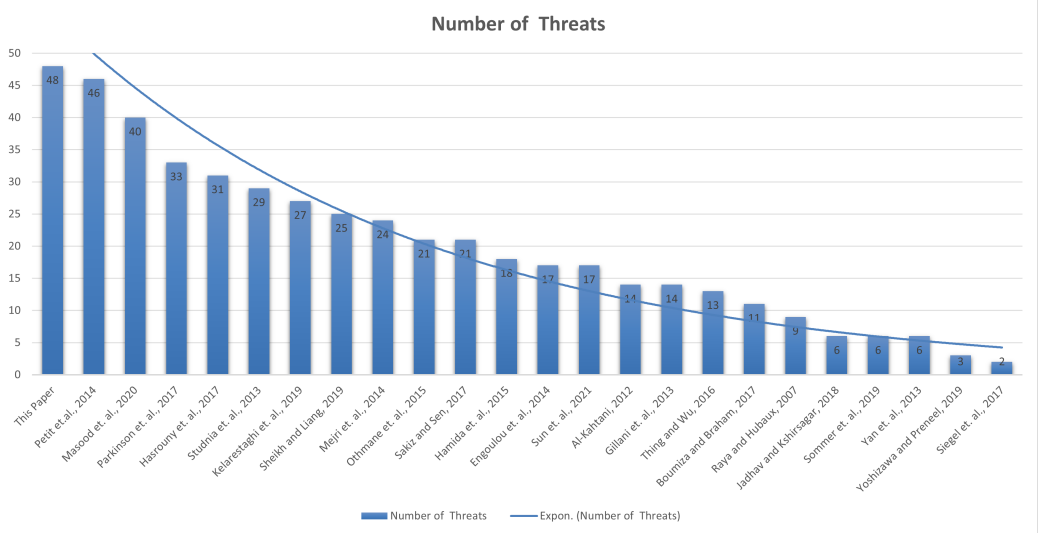

Figure 8. Number of identified threats from the taxonomy against other papers in the literature. The articles suggested in the figure can be referred from [15–37].

The visual representation clearly shows that the number of threats identified in this paper using the taxonomy surpasses those found in past literature, underscoring the depth and breadth of the current research [15–27,29–33,35–37]. Moreover, the taxonomy addresses all *L* threats but also highlights a gap of 15 *R* threats not yet reported. This shortfall could be due to the advanced nature of these threats, the absence of detection tools in the market, nondisclosure in recognised security frameworks such as *CVE* and *CWE*, or ongoing mitigation efforts within the industry.

Furthermore, the graph indicates that while this paper's contribution to the threat landscape is significant, there is a discrepancy with the *P* use case, where 23 of the identified *L* threats were not observed. This may suggest a lack in the adoption of CCAVs for commercial and pub lic usage or a dearth of research focussing specifically on platooning applications. Thus, while the research has made substantial significance in identifying and categorising potential threats, it also points to the need for continuous and rigorous security assessments to bridge existing knowledge gaps and address emerging vulnerabilities within the domain of CCAVs.

Our research on the threat landscape in three-tier CCAV systems extends beyond the specific implications for platooning applications. This is a foundational study, showcasing the depth of knowledge and research efforts aimed at addressing the security of CCAV applications, with platooning as a primary use case. It is important to note that, as detailed in Table A1, over 60 distinct CCAV applications beyond platooning can be identified. These include critical functionalities, such as 'Turning Movements and Intersection Analysis', 'Queue Warning', and 'Curve Speed Warning'.

The comprehensive approach employed in our study to analyse threats within the platooning context provides a critical approach that can be applied to other CCAV applications. The potential impact of CCAV threats, when exploited by adversaries, can be comprehensively analysed using our findings. The attack mechanisms detailed in Tables A6 and A7 are not confined to platooning, but are indicative of broader security concerns that could affect various aspects of CCAV operations. By extending the application of our research findings and methodologies, future studies can explore and address the security implications in these diverse CCAV scenarios, thereby enhancing the overall security and safety of CCAV systems across different functionalities.

In this research, we set out to thoroughly investigate the threat landscape of CCAVs, with a specific focus on the platooning use case. This comprehensive survey methodically achieved this aim through several key steps: (1) Providing Context with CCAV Technology Background - the research offered a detailed overview of CCAV technology to set the stage for understanding its complexities and the significance of security within this domain; (2) Literature-Based Threat Identification - the survey delved into existing literature to enumerate and categorise potential threats to CCAVs, establishing a theoretical foundation for understanding these vulnerabilities; (3) Real-Life Incident Analysis - the study extended our investigation beyond theoretical threats to include those identified from actual incidents. This approach grounded our research in practical, real-world scenarios, enhancing the relevance and applicability of our findings; (4) Focussing on Platooning-Specific Threats - given the unique characteristics of platooning within CCAVs, we identified and analysed threats that specifically target this application, highlighting its distinct security challenges; (5) Determining Affected Trust Domains - the study categorised the identified threats based on the trust domains they affect, providing a structured view of the impact zones within the CCAV ecosystem; (6) Attack Mechanism Identification: the investigation went further to identify the mechanisms through which these attacks are carried out, offering insights into the operational aspects of these threats; (7) Discussion of Open Challenges - the following section would delve into the open challenges in the field, pointing out areas that require further research and attention. Through these steps, our research has not only explored the current threat landscape for CCAVs, particularly in the context of platooning, but has also laid down a comprehensive foundation for future studies in CCAVs. The following sections further elaborate the implications of our findings for the future research of CCAV security.

8. Open Challenges

Our research indicates that numerous publications have focussed on enhancing the security and privacy of on-board and off-board systems. Solutions have encompassed cryptography, authentication, trust-based mechanisms, pseudonyms, privacy-enhancing techniques, and federated learning approaches. Public Key Infrastructure (PKI) utilising digital signatures, encryption, and certificates through TAs or Centralised Authorities (CA) have also been employed [82]. However, challenges still remain, which are discussed below.

8.1. Addressing Security Concerns in the Lifecycle Management of CCAV Systems

Threats in CCAV systems involve any malicious action that deviates the system from its intended behaviour. Onboard security is paramount, comprising control system security, onboard data protection, and secure lifecycle management. To secure control systems, sensing, actuation, and internal processing modules must be considered. Sensing modules should accurately capture data and handle unforeseen events, while actuators need to implement data inputs quickly and accurately. The internal processing module should ensure availability, avoid delays, maintain data authenticity and integrity, handle data formats, and correlate multiple data streams. Complexity arises when hardware and software updates are required for CCAVs. Remote software updates through the cloud or edge cloud can introduce security issues if the application is malicious or unauthenticated. Thus, secure lifecycle management (Table 6) is crucial. Continuous lifecycle management ensures the examination of security requirements throughout the vehicle application phase, including platooning, for the safe operation of CCAV control systems [83].

Table 6. CCAV system lifecycle management.

Starting Secure	Running Secure	Staying Secure
Root of trust establishment	Trustworthy system	Integrity protection
Hardware and software	Validated inputs	Update through trusted and authenticated source
Integrity policies	Detection and prevention runtime attacks	Updating only authorised modules
		Freshness in update process
		Maintaining trustworthiness through re-establishment of updated components

8.2. Enhancing CCAV Security through Adaptive Threat Modeling and Dynamic Risk Assessment

With resource-constrained sensors and actuators, CCAVs must be capable of swiftly processing large volumes of data. Due to growing system vulnerabilities, a determined adversary might use internal or external attack surfaces to alter an expected behaviour. Additionally, when connected to a range of networks, the attack surfaces increase. Therefore, it is critical to regularly identify security requirements for each function and process. Present threat modeling and risk assessment methodologies exhibit a static nature, thereby limiting their utility in supporting sustainable decision-making when it comes to prioritising threats within dynamically evolving threat landscapes. To satisfy security requirements, a systematic threat analysis and risk assessment (TARA) must be performed continuously. These security requirements must be followed on a consistent basis throughout the vehicle's lifecycle as well. This demonstrates the critical need for adaptive threat modeling and dynamic risk assessment methodologies in protecting the CCAV system from emergent risks during the vehicle application phase [15,17,23,29,83–86].

8.3. Securing a Resource Constrained CCAV System

With a long life expectancy and deteriorating on-board computer capabilities, CCAVs are designed to be secure and adaptable to changing needs over time. This is a difficulty in terms of guaranteeing the security of systems supporting V2X-based CCAV applications that need instantaneous responses over time [87]. IEEE, ETSI, and SAE standards all require cryptographic systems based on elliptic curve encryption and authentication for V2X communication [40,43]. However, encryption and authentication overheads over vehicular messages impose additional computational and communication latency on vehicular systems. This is because existing cryptographic mechanisms do not meet the performance requirements of CCAVs. Latencies are introduced by security-related characteristics, such as encapsulation and decapsulation, and such delays have been understudied. As such, low-overhead cryptographic techniques, algorithms or protocols is required in such systems. Additionally, different CCAVs would have distinct system architectures and data processing methods, further adding to the complexity and increasing latencies. As a result, there is a scarcity of comprehensive research which can be used to recommend effective security solutions.

The field of self-protecting software and adaptive systems is seeing rapid growth. The authors in [88] explores self-protecting software as a means of achieving adaptive and opportunistic security. These are classified as "reactive" or "proactive", respectively. While reactive software/systems identify malicious data packets or recurring failures, proactive software/systems anticipate and address security limits and issues in advance. Rather than relying on static security mechanisms for CCAVs, using "Proactive" tactics with adaptive security procedures would be a more appropriate topic to investigate in light of the limits outlined above. An exciting field of could focus on the adaptive security mechanisms for minimising balancing computational and communication latency in order to provide reliable communication in V2X scenarios.

8.4. Developing a Multi-Dimensional Approach to Strengthening CCAV Systems

To enhance the trustworthines of CCAVs, numerous cryptographic and authentication strategies, including context-awareness, relevance, zone, and distance-based encryption and authentication methods have been introduced [71]. Further studies have delved into leveraging vehicle social networks, using centrality and communication history to build 'trustworthiness'. While these strategies predominantly rely on public keys, digital certificates from a Certificate Authority (CA), and message encryption, they remain susceptible to breaches and have questionable system reliability. Additionally, they often fall short in adapting to rapidly changing networked systems. Amidst this complexity, a universal definition of trustworthiness remains elusive, and no comprehensive trustworthy measurement framework or metrics currently exist. Moreover, a considerable portion of research oversimplifies trustworthiness, viewing adherence to security standards alone as the cornerstone. However, this perspective is potentially myopic, overlooking other pivotal factors such as privacy. To remedy these challenges, it is imperative to delineate adequate parameters for trust mechanisms in CCAV, considering the system during the design and operation phase. This approach should holistically embrace security, privacy, resilience, reliability, robustness, and ethics. Such exploration sets the stage for a multifaceted approach to trustworthy CCAV systems, contributing substantially to the broader ITS and IoT landscape.

8.5. Embracing Zero Trust Principles for Enhanced Security in Dynamic Environments

In conventional cybersecurity scenarios, particularly with legacy systems that lack V2X connectivity, the emphasis has been on safeguarding static network boundaries, but the dynamic nature of CCAVs operating in platoon configurations introduces new complexities. Specifically, predicting measures and consistently conforming to security requirements from design through operation becomes a formidable task. As establishing trust in such environments remains a frontier in research, a shift towards the zero-trust approach has emerged. This approach pivots on a foundational scepticism towards all network components, physical assets, and users, mandating distinct authentication and authorisation processes for every session, irrespective of entity type—be it human, vehicle, or related devices such as smartphones. At its core, Zero Trust focuses on protecting specific resources, such as individual sessions or processes, rather than broad network segments, highlighting the evolving belief that a resource's security is not exclusively related to its network location or boundaries. Even with its potential, the principles of Zero Trust Architecture (ZTA) are still in their infancy, especially in cyber-physical system contexts and more so in CCAVs. Institutions such as the National Institute of Standards and Technology (NIST), along with academic and industry stakeholders, are in the early stages of exploring and developing ZTA. For platoons, adopting ZTA, increasing scepticism with increased authentication and authorisation dynamically may be promising but may challenge the limited computational resources [89]. ZTA, with its innovative approach, stands out as a potential solution to meet these pressing security needs effectively; however, further research is required.

8.6. Assessing, Prioritising, and Mitigating Privacy Risks

CCAVs have complex privacy concerns, especially when Personally Identifiable Information (PII) is communicated across systems. A methodical, multi-layered approach is vital not only to understanding privacy risks associated with CCAVs but also to developing proactive strategies within privacy-by-design principles. Existing literature presents unstructured methodologies, poorly informing stakeholders whilst challenging decision-making processes for privacy assurance. Thus, there is an emerging demand for refined privacy modeling and assessment. Privacy Impact Assessment (PIA) has been proposed as a potential solution, which could enhance stakeholder confidence and provide verifiable compliance with modern privacy standards [90,91]. Within the CCAVs and platooning, PIA could be considered to be a central tool for assimilating advanced privacy solutions such as differential privacy, federated learning, and homomorphic encryption; however, this is still in its early developmental phase. As such, it is important for both academia

and industries to develop standards and methodologies for ensuring privacy in CCAV applications systematically.

8.7. Addressing Data Scarcity

In the rapidly evolving landscape of CCAV, the integration of machine learning and AI technologies has ascended to a paramount significance. The sheer magnitude of data inherent to these systems necessitates efficient processing and analysis, compelling CCAVs to lean heavily on the capabilities of edge clouds and centralised cloud platforms [92]. An important challenge, however, remains the dearth of accessible real-world data. This scarcity often stems from either its sheer non-existence or organisational resistance rooted in privacy concerns. In this intricate situation, synthetic data have emerged as part of important research where AI models can generate high-fidelity data, presenting a viable solution [93]. It addresses a variety of challenges encountered during the training and testing phases of machine learning tools and AI frameworks, notably in ensuring data privacy, minimising inherent biases, and supplementing the pool of labeled datasets requisite for effective training. Yet, even as the merits of synthetic data in bolstering CCAV application security become evident, the automotive industry's research endeavours in this domain appear somewhat constrained. There remains an urgent need to delve deeper into the mitigation strategies against presentation attacks and other security concerns using synthetic data. We conclude this paper by reflecting on the challenges identified through an examination of the threat landscape for CCAVs, specifically focusing on the platooning use case, as revealed by our comprehensive survey. This will enable future advancements in these areas, as outlined in Table 7, which we have discussed.

Table 7. Future Works.

Future Works	Description
Advancements in Secure System Lifecycle Management	• Development of specialised security *protocols* tailored for CCAV applications is important, especially during software and hardware updates • Investigating methods for ongoing assessment and *monitoring* of security measures throughout a vehicle's lifecycle is crucial for identifying and mitigating evolving threats.
Evolution of Threat Modeling and Risk Assessment methods	• Development of *adaptive threat modeling and dynamic risk assessment* frameworks, modelts and methods for evolving threat landscape of CCAVs is required to preemptively address emerging threats. • Research on methods to utilise AI and machine learning for real-time security threat assessment and response to enhancing the ability to rapidly identify and mitigate threats is required.
Optimising Security for Resource-Constrained CCAVs	• Research on security mechanisms and lightweight cryptographic techniques that are secure yet resource-efficient for CCAVs is required.
Establishment of Multifaceted Trust Mechanisms and Framework for CCAVs	• Research focusing on developing methods to empirically validating trust frameworks that encompass pillars such as security, privacy, ethics, reliability, resilience, and robustness to ensure their practical applicability and effectiveness in real-world scenarios is required.
Implementing Zero Trust Architecture in CCAVs	• Research on novel solutions that are rigorously tested for resource-constrained CCAVs is required for implementing Zero Trust architecture and its techniques.
Strategies for Mitigating Privacy Risks	• Research focussing on developing and standardising tools specifically for assessing privacy threats and impacts in CCAV environments to strengthen privacy measures. • Researching on the integration of privacy ensuring schemes such as homomorphic encryption within CCAVs is required.
Addressing Data Scarcity in CCAV Development	• Development of high-quality synthetic datasets is required to enhance AI model training in CCAV applications. • Collaboration between industry and academia to share real-world datasets is required to address both data accessibility and privacy issues is required.

9. Conclusions

To address the aim of this research, this paper presents a comprehensive survey by exploring the threat landscape of CCAVs operating within a platoon. Adhering to the methodology outlined in Section 2, this study has rigorously gathered a comprehensive list of threats, comprising 132 identified from academic literature, 64 derived from real-life incidents, and 22 specifically related to platooning microservices (Tables A2, A6, A7 and A8, Appendix A). To do so, this study formulates an analytical timeline of these threats, and also correlates the threats from the literature and platooning microservices.

From our results, we map a detailed attack taxonomy using threats from the literature, real-life incidents, and the platooning use case. Based solely on this taxonomy, we narrow down the total threats to 48 categorically, surpassing the number of threats previously identified in the literature (Figure 8). For defending against emerging threat landscape, this study identify immediate security challenges for further research in CCAV systems. This paper is novel in the field of CCAV, enhancing threat analysis by intertwining insights from the literature and real-life incidents, specifically focussing on platooning use case, resulting in the definition of important trust domains and attack vectors.

This work lays the foundations for highlighting the importance of a dynamic and systematic threat analysis of the evolving CCAV systems. Protecting CCAVs requires transitioning from static defences to dynamic, multifaceted security strategies. Embracing continuous security lifecycle management, adaptive threat modeling, and Zero Trust principles is crucial, balanced with optimal solutions for resource-constrained computation. Identified challenges within the CCAV ecosystem, particularly with hardware–software advancements, signal an urgent need for a more continuous and rigorous threat analysis.

This study also acknowledges the methodological constraints, including reliance on secondary data with potential biases, the absence of empirical validation, and the rapid evolution of CCAV technology outpacing this research scope. Thus, we recommend conducting a systematic, in-depth study using threat analysis methods to capture the intrinsic hardware-software interaction in the broader CCAV ecosystem. This would offer valuable insights for informed decision making in risk management using the defined trust domains. This critical exploration, pivotal for enhancing system-wide CCAV security, safety, reliability, resilience, and robustness, necessitates collaborative engagement across academic, industrial, and regulatory stakeholders. This shift demands collective and proactive efforts from stakeholders to ensure secure, efficient, and privacy-aware CCAVs within intelligent transportation ecosystems.

Author Contributions: Conceptualisation, C.M. and A.T.S.; Methodology, A.T.S.; Software, A.T.S.; Validation, C.M., G.E. and M.D.; Formal Analysis, A.T.S.; Investigation, A.T.S.; Resources, A.T.S.; Data curation, A.T.S.; Writing—Original Draft Preparation, A.T.S.; Writing—Review & Editing, A.T.S., G.E., C.M. and M.D.; Visualisation, A.T.S.; Supervision, C.M. and M.D.; Project Administration, C.M. and M.D.; Funding Acquisition, C.M. and M.D. All authors have read and agreed to the published version of the manuscript.

Funding: The work presented has been funded by EP/R007195/1 (Academic Centre of Excellence in Cyber Security Research—University of Warwick); EP/N510129/1 (The Alan Turing Institute); and EP/S035362/1 (PETRAS National Centre of Excellence for IoT Systems Cybersecurity) and EP/R029563/1 (Autotrust).

Data Availability Statement: The data presented in this study are available on request from the corresponding author, A.T.S. The data are not publicly available due to the confidentiality of the research undertaken.

Acknowledgments: The authors would also like to thank Nicola Beech and Jagdish Hariharan for proofreading this work.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, and in the decision to publish the result.

Appendix A

Table A1. CCAV applications modified from [2].

CCAV Applications		
V2I Safety	**Environment**	**Mobility**
Red Light Violation Warning	Eco-Approach and Departure at Signalised Intersections	Advanced Traveller Information System
Curve Speed Warning	Eco-Traffic Signal Timing	Intelligent Traffic Signal System
Stop Sign Gap Assist	Eco-Traffic Signal Priority	Signal Priority (transit, freight)
Stop Weather Impact Warning	Information Disclosure	CCAV platooning
Reduced Speed/Work Zone Warning	Connected Eco-Driving	Mobile Accessible Pedestrian Signal System
Pedestrian in signalised crosswalk warning	Wireless Inductive/Resonance Charging	Emergency Vehicle Preemption
V2V Safety	Eco-Lanes Management	Dynamic Speed Harmonisation
Emergency Electronic Brake Lights	Eco-Cooperative Adaptive Cruise Control	Queue Warning
Forward Collision Warning	Eco-Speed Harmonisation	Cooperative Adaptive Cruise Control
Intersection Movement Assist	Eco-Cooperative Adaptive Cruise Control	Incident Scene Pre-Arrival Staging
Left Turn Assist	Eco-Traveler Information	Guidance for Emergency Responders
Blind Spot/Lane Change Warning	Eco ramp metering	Incident Scene Work Zone Alerts for Drivers and Workers
Do not pass warning	Low-emission zone management	Emergency communications and evacuations
Vehicle turning right in front of bus warning	AFV Charging/Fueling Information	Connection Protection
Agency Data	Eco-Smart Parking	Dynamic Transit Operations
Probe-based pavement maintenance	Dynamic Eco-Routing	Dynamic Ridesharing
Probe-enabled traffic monitoring	Decision Support System	Freight-specific Dynamic Travel planning and performance
Vehicle classification based traffic studies	**Road Weather**	Drayage Optimisation
Turning Movement and Intersection Analysis	Motorist Advisories and Warnings	**Smart Roadside**
Origin Destination Studies	Enhanced MDSS	Wireless Inspection
Work zone traveller information	Vehicle Data Translator	Smart Truck Parking
	Weather Response Traffic Information	

In this table, items in bold represent key categories within each CCAV application area.

Table A2. Platooning attacks classified based on the platooning incident code (PL-IC), identified threats, Impacted CCAV Trust Domain (TD), Impacted Edge Trust Domain (TF), STRIDE threats, Impacted platoon microservices, threat description. The labels are: Forming (F), Managing (M), Joining (J), Leaving (L), Merging (Mg), Splitting (S), Ending (E), and Changing Leader (CL).

CCAV Platooning Attacks												
PL-IC	**Threat**	**CCAV TD**	**Edge TD**	**STRIDE**	**F**	**M**	**J**	**L**	**Mg**	**S**	**E**	**CL**	**Threat Description**
PL-IC1	Covert Channel	V-TD1, V-TD3, V-TD9, V-TD10, V-TD11	E-TD1, E-TD2, E-TD5, E-TD6, E-TD12	S, T, D, E	✓	✓	✓	✓	✓	✓	✓	✓	• In vehicle platooning: Covert channel attacks occur when packets are transferred between vehicles without proper authentication, exploiting communication channels not intended for data transfer and compromising communication and algorithms. • Two types of covert channel attacks: Timing-based attacks alter the timing of packets to transfer data, while storage-based attacks hide data in shared resources such as storage locations.
PL-IC2	Black Hole	V-TD1, V-TD3, V-TD10, V-TD11	E-TD1, E-TD2, E-TD5, E-TD6, E-TD12	S, T, D, E	✓	✓	✓	✓	✓	✓	✓	✓	• The attacker in vehicle platooning seeks to force packet collisions, leading to dropped packets and a loss of communication for some platoon members. • This results in a violation of the transmitted information's integrity. • The attacker can use this method to selectively prevent some or all traffic within the platoon, deciding which nodes can communicate and when.
PL-IC3	Worm Hole	V-TD1, V-TD10	E-TD1, E-TD2	T, D, E		✓	✓	✓	✓	✓	✓	✓	• Wormhole attack: A private communication link between two non-neighbouring vehicles. • Exclusion of vehicles: The attack results in the exclusion of vehicles between the two attackers. • Threat to platooning: The wormhole attack damages the availability of the vehicle platoon and represents a security threat.
PL-IC4	Packet dropping	V-TD1, V-TD3, V-TD10, V-TD11	E-TD1, E-TD2, E-TD5, E-TD6, E-TD12	S, T, D, E	✓	✓	✓	✓	✓	✓	✓	✓	• In this type of attack, the attackers act as forwarders for dropping packets. • The attackers either drop all packets, referred to as black hole attack or drop packets selectively, which is known as gray hole attack
PL-IC5	Jamming Attack	V-TD1, V-TD10	E-TD1, E-TD2	D		✓	✓	✓	✓	✓	✓	✓	• Jamming attacks target the Physical Layer by flooding channels with noise, causing disruption in platoon communication. • Attacker can target individual messages or block specific channels to break up the platoon, potentially leading to collision. • Each time the platoon breaks up or adjusts for safety, it loses the benefits of platooning.

Table A2. *Cont.*

CCAV Platooning Attacks													
PL-IC	**Threat**	**CCAV TD**	**Edge TD**	**STRIDE**	**F**	**M**	**J**	**L**	**Mg**	**S**	**E**	**CL**	**Threat Description**
PL-IC6	Jamming and Spoofing Sensors	V-TD1, V-TD4, V-TD11	E-TD1, E-TD2, E-TD5, E-TD12	S, T, D	✓	✓	✓	✓	✓	✓	✓	✓	• Jamming attacks target the Physical Layer by flooding channels with noise, preventing platoon communications. • Jamming attacks can cause platoon members to lose communication and potentially lead to accidents. • Sensor authenticity and availability can be compromised through malware or direct attacks, leading to false sensing.
PL-IC7	False Data injection	V-TD1, V-TD10, V-TD11	E-TD1, E-TD2, E-TD5, E-TD12	T, D	✓	✓	✓	✓	✓	✓	✓	✓	• Fake data injection attack is when a malicious node creates and transmits fake messages into the network. • The attacker must create a packet in the same format as the network it is transmitting into, either by being a network member or copying a message format. • Such attacks disrupt platoons, causing degradation in stability and affecting traceability, data verification, and integrity.
PL-IC8	Eaves-dropping	V-TD1, V-TD11	E-TD1, E-TD12	I									• Eavesdropping is the act of monitoring and logging the communications of a network • In platooning, the attacker can see the beacon used by members to maintain formation • The goal of the attack is to gain information about the platoon and member vehicles, which can then be used for further attacks such as Replay or Sybil.
PL-IC9	Data collection and Information theft	V-TD1, V-TD11	E-TD1, E-TD12	I									• Information transmitted by vehicles in a platoon network can contain sensitive information. • The information transmitted by the beacon can be used for various purposes, both for improving the platoon service or for criminal targeting of individual vehicles. • The ownership of the information transmitted is a current issue, with different entities (driver, fleet manager, platooning enabling company) having legal responsibilities.
PL-IC10	Location Disclosure	V-TD1, V-TD11	E-TD1, E-TD12	I									• Location tracking attacks can reveal the position of a vehicle by intercepting GPS location information or by extracting it from the beacon. • Interception of GPS information breaches privacy of the targeted vehicle. • Extraction of location information from the beacon breaches confidentiality among platoon members who should remain anonymous.

Table A2. *Cont.*

CCAV Platooning Attacks													
PL-IC	**Threat**	**CCAV TD**	**Edge TD**	**STRIDE**	**F**	**M**	**J**	**L**	**Mg**	**S**	**E**	**CL**	**Threat Description**
PL-IC11	Man-in-the-Middle	V-TD1, V-TD10, V-TD11	E-TD1, E-TD2, E-TD5, E-TD9, E-TD6, E-TD12	T, D	✓	✓	✓	✓	✓	✓	✓	✓	• Attacker takes control of communication between two trucks in the truck platoon. • Violates integrity, authenticity, and non-repudiation issues in truck platoons. • Attacker acts as middle man between sender and receiver trucks.
PL-IC12	Tunnel Attack	V-TD1, V-TD6, V-TD10, V-TD11	E-TD1, E-TD3, E-TD12	S, T, E	✓	✓	✓		✓			✓	• Attacker copies the GPS transmission before replaying them, slowly moving the position away from the vehicle's actual location. During this, the strength of the fake signal must be stronger than the original one as GPSs are often set up to take the strongest signal as the true original message
PL-IC13	Fake Positioning	V-TD1, V-TD11, V-TD4, V-TD10	E-TD1, E-TD2, E-TD5, E-TD12	S, T		✓	✓	✓	✓	✓	✓		• Attacker transmits fake position coordinates into the platoon network. • This misleading information will change the perceived order of the platoon.
PL-IC14	Fake Manoeuvering	V-TD1, V-TD11, V-TD4, V-TD10, V-TD9	E-TD1, E-TD2, E-TD5, E-TD12	S, T, D, E		✓	✓	✓	✓	✓			• Fake entrance attacks can cause gaps in platoons, reduce the number of member vehicles, and reduce platoon efficiency. • Fake leave and split requests can break up platoons, providing an opportunity for the attacker to become the leader and target specific vehicles. • Fake manoeuvre attacks can damage the integrity and availability of security characteristics, leading to a denial of service attack on vehicles.
PL-IC15	Session Hijack	V-TD1, V-TD10, V-TD11	E-TD3, E-TD5, E-TD10	S, D	✓	✓	✓	✓	✓	✓	✓	✓	• Attacker spoofs IP address of a legitimate truck to block other trusted trucks, resulting in session hijacking. • Genuine truck whose IP address was used becomes unavailable for the session. • Attacker takes control of the session among trucks, leading to violation of security characteristics such as Availability and Integrity.

Table A2. *Cont.*

CCAV Platooning Attacks													
PL-IC	**Threat**	**CCAV TD**	**Edge TD**	**STRIDE**	**F**	**M**	**J**	**L**	**Mg**	**S**	**E**	**CL**	**Threat Description**
PL-IC16	Malware or Ransomware	ALL	ALL	S, T, R, I, D, E	✓	✓	✓	✓	✓	✓	✓	✓	• Malware attacks can have catastrophic consequences to platoons, such as shutting down the whole network and preventing users from platooning. These attacks can compromise the availability, confidentiality, and privacy of the platoons. • Malware can infect a vehicle's On-Board Computer through various interfaces, including the OBD port, CD drive, USB interface, Bluetooth, and wireless communication network link. The malware can be installed by infecting multimedia files, the OBD port, or by sending the malware through Bluetooth or other wireless communication links.
PL-IC17	Repudiation attack	ALL	E-TD1, ETD2, E-TD5, E-TD12	S, R, E	✓	✓	✓	✓	✓	✓	✓	✓	• Repudiation attacks aim to confuse the network by denying the receipt of messages during disputes over messages. • This type of attack can lead to the system assigning the same identity to multiple vehicles in platoons, making it difficult for network members to distinguish between members. • As a result, the attacker is able to manipulate the platoon and pretend to be other vehicles.
PL-IC18	Flooding	V-TD1, V-TD3, V-TD10, V-TD12	E-TD1, E-TD2, E-TD5, E-TD6, E-TD3, E-TD12	T, D	✓	✓	✓	✓	✓	✓	✓	✓	• Flooding attacks on platoons aim to exhaust network resources and prevent communication. • There are two types of flooding attacks: data flooding and routing control packet flooding. • Data flooding involves transmitting too many packets for the network to handle. Routing control packet flooding involves sending routing requests to nearby vehicles, breaking up the platoon communication and compromising data verification and network availability.
PL-IC19	Replay attack	V-TD1, V-TD4, V-TD9, V-TD10, V-TD11	E-TD1, E-TD6, E-TD10, E-TD11	S		✓		✓	✓	✓			• Replay attacks in platoons involve an attacker replaying old messages into the network, causing instability and reduced efficiency. • This type of attack affects the privacy and integrity of the platoon. • The replayed messages can result in significant gaps or oscillation within the platoon, leading to decreased efficiency.

Table A2. *Cont.*

CCAV Platooning Attacks													
PL-IC	**Threat**	**CCAV TD**	**Edge TD**	**STRIDE**	**F**	**M**	**J**	**L**	**Mg**	**S**	**E**	**CL**	**Threat Description**
PL-IC20	Impersonation Attack	ALL	E-TD1, E-TD2, E-TD5, E-TD12	S, E	✓	✓	✓	✓	✓	✓	✓	✓	• Impersonation attack: In this type of attack, the attacker convinces the victim trucks that the messages being sent are from a genuine truck, when in fact they are corrupted. • The attacker captures and analyses application services, changes its identity to match that of the original truck, leading to the circulation of false information in the network.
PL-IC21	Illusion Attack	V-TD1, V-TD3, V-TD4, V-TD11	E-TD1, E-TD3, E-TD5, E-TD12, E-TD6, E-TD11	S, T	✓	✓	✓	✓	✓	✓		✓	• A malicious node transmits false or misleading information into the network. • The malicious node creates fake messages about traffic conditions, driving conditions, and members. • The attack affects the MAC layer and disrupts the cooperation of MAC protocols, potentially causing traffic jams, accidents, a decrease in performance of the platoon, degradation of integrity, and data verification within the platoon network.
PL-IC22	Sybil Attack	V-TD1, V-TD10, V-TD6, V-TD11	E-TD1, E-TD2, E-TD5, E-TD6, E-TD11, E-TD12	S, R, D, E	✓	✓	✓		✓				• Attacker creates ghost vehicles upon entering the platoon network and tries to have these accepted into the platoon. • When the ghost vehicles are part of the platoon, they can destabilise the platoon by creating gaps. The leader will also think there are more vehicles than there are, stopping new vehicles from joining. • The attacker can take it a step further and try to take control of the platoon off the leader using the ghost vehicles.

Table A3. CCAV trust domains.

CCAV Reference Architecture		
Trust Domain	**Data Process**	**Description**
V-TD1: Wireless Communication	Data Transmission	CAVs communicate with the Edge Cloud, other cars, and CAVs, possible technologies linked to road users, infrastructures, and radio stations on a frequent basis, depending on the receiver and transmitter's position and vicinity. DSRC, 5G, 4G/LTE, and other protocols may be used for sharing data, depending on the application.
V-TD2: Infotainment	Physical Interaction and Data Transmission	It is a group of hardware and software components installed in automobiles that offer audio and visual entertainment. It began with radios with cassette or CD players and has expanded to include navigation systems, video players, USB and Bluetooth connection, internet, and WiFi. Examples include CarPlay and Android Auto. The internal components (wireless communication module, I/O ports and data storage) can transmit data to this module
V-TD3: Data Storage	Database Access	Vehicles would need storage for data related to audio, video, maps, firmware and its versions, and vehicle status. These records are partitioned and securely stored.
V-TD4: Vehicle Sensors	Data Processing	Vehicles are often equipped with a plethora of sensors that monitor the vehicle's motion dynamics and vehicle system. GNSS, LIDAR, RADAR, and cameras are all important sensors for CAVs. Additionally, sensors such as tyre pressure monitoring sensors, light sensors, parking sensors, wheel and vehicle speed sensors, and others are considered in this study.
	Physical Interaction	The on-board sensors may be exposed to environment specific threats,
V-TD5: Physical Input/ Outputs	Physical Interaction	This module refers to the physical inputs and outputs on the device, such as the USB port and the on-board diagnostic port (OBD-II), Type1-4 battery chargers. It is difficult to exploit these ports since they need physical access.
V-TD6: Monitoring	Data processing	This module is used to describe the vehicle's monitoring function. Here, the vehicle's operation is verified against its specifications, its history is verified, and the vehicle's maintenance is documented and logged. A good commercial example is the black box.
V-TD7: HMI	Phy. interaction, data processing & trans.	The Human–Machine Interface (HMI) is a collection of hardware and software elements that enables an individual to engage actively with the CAV system. It may be used as a user interface for steering wheels equipped with sophisticated on-board displays.
V-TD8: Energy System	Physical Interaction	The on-board energy system may be vulnerable to environmental challenges. It mainly consists of batteries and a fuel tank (petrol or diesel).

Table A3. *Cont.*

CCAV Reference Architecture		
Trust Domain	**Data Process**	**Description**
V-TD9: Actuators	Data Processing	This module discusses components that have the potential to influence the physical environment. This includes adjusting the wheel speed and angle, activating the brakes, air conditioning, and windows, as well as locking the doors and trunk.
	Physical Interaction	Physical components receive their energy unit to interact with the environment
V-TD10: Data Analysis	Data Processing	This module is in charge of conducting analysis on the data that have been saved. This might be for data localisation, object recognition, sensor fusion and analysis, action engine decision-making, vehicle control automation, warning, and basic safety message analysis, as well as vehicular applications.
	Physical Interaction	Physical components receive their energy unit to interact with the environment
V-TD11 Devices and Peripherals	Data Processing and Physical interaction	Smartphones, Bluetooth devices, laptops, and desktop computers are all examples of devices and peripherals. Admins, users, and operators would use these devices to communicate with CCAV and devices to use the system. These are additional methods via which an adversary may breach the system. COHDA units are used to represent roadside infrastructure. These devices would be utilised by traffic controllers, CAVs, and other edge devices to carry out ITS-based prompts.

Table A4. Edge cloud trust domains.

Edge Cloud Reference Architecture		
Trust Domain	**Data Process**	**Description**
E-TD1: Wireless Communication	Data Transmission	The communication module presented here is expected to establish wireless connections with nearby automobiles, cloud technologies, RSI, and other peripheral devices through a cellular network or DSRC. They are also linked through fibre optic cables to the Wide Area Network (WAN).
E-TD2: Microservices	Data Processing and data transmission	The microservices module is in charge of offering services that are composed of multiple services. They are well known for providing unique services through facilitating scalability and testing. For example, intersection management.

Table A4. *Cont.*

Edge Cloud Reference Architecture		
Trust Domain	**Data Process**	**Description**
E-TD3: API	Data transmission and interaction	Application Program Interfaces (APIs) are used by users and software modules to get access to a specific service.
E-TD4: Physical I/O	Phy. interaction & data trans.	Connection to the Edge infrastructure is made possible via the Physical IO ports. Physical security mechanisms should be used to protect these ports from physical attack. Users connecting over these ports should be properly authenticated, and digital records of these connection attempts should be maintained.
E-TD5: Process & Data Analysis	Data Processing	Actuators on the edge may have an effect on the surroundings. The edge may be capable of altering the behaviour and security of cars.
E-TD6: Data Storage	Database access	Data storage at the Edge will be centralised in a single piece of memory hardware. Due of its exposure to manipulation, it is critical to provide safeguards such as encryption, access control, and authentication to the whole disc to prevent threats.
E-TD7: Energy System	Physical Interaction	Electricity will be used to power edge systems. Alternative energy sources (such as batteries and renewable energy sources such as solar) may be employed in places where supplying electricity is difficult.
E-TD8: Actuators	Physical Interaction	Actuators on the edge may have an effect on the surroundings. The edge may be capable of altering the behaviour and security of cars.
E-TD9: Monitoring	Data Processing	Both the Edge and the Cloud will need to keep track of their activities. This enables analysts to comprehend why a certain series of events happened. They will also be required to comprehend the system's performance characteristics.
E-TD10: Sensors	Data Processing and transmission	The Edge is equipped with both internal and exterior sensors. Individual devices inside an edge may have sensors that provide information about the status of the environment within the systems. Meanwhile external sensors may provide information about the edge of its environment, such as its surroundings.
E-TD11: Devices	Data Processing and transmission	Smartphones, Bluetooth devices, laptops, and desktop computers are all examples of devices and peripherals. Admins and operators would use these devices to communicate with the edge in order to maintain or operate the system. These are additional methods via which an adversary may breach the system.
E-TD12: Roadside Infrastructures	Physical interaction, data processing and transmission	COHDA units are used to represent roadside infrastructure. These devices would be utilised by traffic controllers, CAVs, and other edge devices to carry out ITS activities.

Table A5. Cloud trust domains.

Cloud Reference Architecture		
Trust Domain	**Data Process**	**Description**
C-TD1: Wireless Communication	Data Transmission	Cloud communication presents a significant challenge due to the need for advanced scalability, performance, dependability, durability, and resilience. To achieve optimal results, the cloud must feature a sophisticated architecture consisting of multiple edge clouds interconnected via multiple gateways, operating with maximum efficiency.
C-TD2: Data analysis	Data processing and data transmission	Advanced data analysis in the cloud due to large data volume enables various functionalities such as traffic control and timely distribution. The cloud predicts future trends by evaluating data from edge requests.
C-TD3: Microservices	Data processing and data transmission	The microservices module is responsible for delivering services comprised of multiple individual services. It is renowned for its ability to provide unique services while promoting scalability and ease of testing, for example, Intersection management.
C-TD4: APIs	Physical Interaction and data transmission	Application Program Interfaces (APIs) are used by users and software modules to get access to a specific service.
C-TD5: Data storage	Data Processing	Edge data storage will be centralised in memory hardware. Given its susceptibility to manipulation-based attacks, it is imperative to implement security measures such as encryption, access control, and authentication to secure the entire disk. The Edge's actuators can impact the environment and have the potential to modify the behavior and security of vehicles.
C-TD6: Monitoring and Logging	Data Processing	Cloud-based decisions made while monitoring the environment, traffic, and other characteristics are saved for future verification. This would allow assessment in the event of a system anomaly or real-world mishap. This is a characteristic of accountability.
C-TD7: Physical I/O	Physical Interaction	Connection to the Cloud infrastructure is made possible via the Physical IO ports. Traffic Operators connect over these ports to access, update, create, delete, and maintain services. Such personnel should be properly authenticated, and digital records of these connection attempts is to be maintained.
C-TD8: Energy Systems	Physical Interaction	Cloud data storage is vulnerable to natural disasters, power outages, cyber attacks, and human errors that can cause data loss and breaches. Energy providers must implement security measures, backups, and redundancies with disaster recovery plans whilst being informed on current threats.

Table A6. CCAV threats.

Trust Domain	Entry Point	Threat Description	Impact
V-TD1: Wireless Communication (Wifi, Cellular, 5G/LTE)	Wireless Communication (Wifi, 5G/LTE)	• Spoofing wireless communication protocol • Jamming wireless communication channel [72,94–96] • A malicious adversary/bot may gain additional privileges [97–99] • MITM in wireless communication (Frame injection, Data replay, Brute force) [12,25,33,98–103]	• An adversary could alter the code or file system of a wireless communication module, compromising its integrity. They could also disrupt communication, thereby compromising availability. • An adversary may jam the specific channel or the environment may influence the signals • An adversary user may gain privileges to perform network propagation • Running traditional man-in-the-middle attack tools on an suspicious twin node to intercept TCP sessions (compromising confidentiality)
	Long-range cellular wireless access [104]	• Long-range wireless channels cellular access using voice, 3G: This can be executed by reverse engineering protocol such as AqLink of the on-board telematics system [72] • To exploit this flaw, one must first authenticate in order to establish a call timeout value long enough to send a payload of suitable length. • Remote access • Practical attack [97] • Scalability is high	• Changes the voice timeout from 12 to 60 s, then re-calls the automobile and attacks the newly discovered buffer overflow issue. • Instructing the car to play a pre-programmed tune using the phone's microphone
V-TD2: Infotainment, V-TD7: HMI	• Primary infotainment ECU (head unit) • Telematics Control Unit (T-Box)	• Physical access to the head unit through OBD an CAN bus—Code accessed through interface or Bus system, internal data to maliciously inject code • Later remote access to both head unit and t-box • Proximity—Physical Access with possibility for remote access • Practical attack [79,94,99,101,105–113] • Scalability is small	• Indirect physical channel leading to complete control of vehicle system. • Adjust color of interior led lights • show photos on the infotainment system [78] • Firmware updates [79] • Access to CAN bus and other gateways to perform alter electric window lift system, warning lights, airbag control system, and gateway ECUS [114]
	• CD Reader	• CD-based firmware update—Peer-to-peer exchange of media files. Exploitation of firmware present in the media player to execute arbitrary code leading to buffer overflow attack [75] • Proximity—Physical Access with possibility for remote access • Practical attack • Scalability is small	• Formatted CD due to which the system can be completely flashed with any adversarial data
V-TD3: Data Storage	• Firmware • Firmware Update • Debug info. • Local Dynamic Map • Software [101,106,115]	• Inject fabricated frames in memory, e.g., blurry frames, wrong tags • Amend firmware to produce fabricated frames leading to creation and deletion of point cloud or frames • Deter/accelerate/delay status and information of modules • Inject malicious coordinates to places, replay of frames, Byzantine attack • Proximity—Remote access [116] • Simulated attack [116] • Scalability is high [100,106,109,111,116,117]	• False warnings or services • Removed warnings or services • Delayed warnings or services

Table A6. *Cont.*

Trust Domain	Entry Point	Threat Description	Impact
V-TD4: Vehicle Sensors	Camera [104]	• RBright (250 lx) and dark (0 lx) environments, with different light sources at multiple distances (50 cm, 100 cm, 150 cm, and 200 cm), presentation attack [118] • Fake environmental conditions [119,120] • Physical access—Close proximity to vehicular camera • Blinding attack [121] • Phantom attack • Practical attack • Scalability is high	• Environmental light considering the light wavelength and distance between the cameras leading to incorrect model recognition [121] • Not able to tune the auto-exposure
	Ultrasonic [121]	• Jamming attack may be accomplished by broadcasting ultrasonic noises that overwhelm the membrane on the sensor • By adjusting the timing of spoofed pulses, an attacker can manipulate the readings of sensor • Practical attack • Scalability is high	• Failing to detect obstacles can lead to collisions in parking or manoeuvreing. • Incorrect data sensed can lead to collisions [121]
	LIDAR [104,122,123]	• Having known the working knowledge of LIDAR and set of transceivers, the attacker receives the LIDAR signal and relays then to next vehicle. • Two Transceivers; LUX 3 uses light with a wavelength of 905 nm, and transceiver B is a photodetector sensitive to this wavelength • Practical attack • Scalability is high	• Incorrect data sensed, which could cause trivial vehicular impacts, leading to incorrect model recognition
	Global Navigation Satellite System (GNSS) [124]	• Jamming may be accomplished by broadcasting powerful signals that overwhelm the GPS receiver • Practical attack • Remote Access • Scalability is high	• Incapable of detecting original signals
	Global Navigation Satellite System (GNSS) [124]	• An attacker sends misleading but plausible GPS signals to deceive GPS receivers on CAVs. The attack starts with signals mimicking those from legitimate satellites, then gradually increases their strength and alters their GPS signals away from the target's actual position [125,126]. • Practical attack [127–129] • Remote Access • Scalability is high	• GPS device processes counterfeited signal
	Auxiliary Sensors: Vehicle's custom telematics features such as UConnect. This includes on-board connectivity feature using wireless sensors and CAN bus vulnerabilities	• Remote access to vehicles communication system with the ability to flash the firmware version [4] • Availability of Uconnect's DBus Port to be open for communication • Remote Access • Practical attack [113,117,130] • Scalability is high	• Incorrect data sensed, which could cause trivial vehicular impacts, leading to incorrect model recognition

Table A6. *Cont.*

Trust Domain	Entry Point	Threat Description	Impact
V-TD5: Physical Input/Outputs	• On-Board Diagnostic Port [131,132] • USB	• Replayed collected CAN packets, capturing each CAV response. The modified CAN packets might then control the vehicle's behaviour. This is enabled with access to the OBD port and with windows PC operating system capable of analysing CAN packets [5] • Direct Physical Access • BUS attack • Practical attack • Scalability is small • Firmware tampering [115]	• Horn: Raise horn continuously • Vehicles brakes: Slam brakes at any speed • Gas: Change speedometer and gas gauze at will • Engine: Cause engine to accelerate • Battery: Prevent car from powering down and/or draining battery • Disable Seat belt notification • Disable power steering or jerk wheel • Turn headlights on or off when left on auto mode
V-TD6: Monitoring	White box and black box attack	• Adversarial input models are more effective at producing successful mispredictions of signboards at a quicker pace and with a larger likelihood of failure[133] • Remote access • Practical lab based attack • Scalability is high	• Mispredictions of signboards
V-TD8: Energy System	Energy and fuel storage, power generation	• Directed energy weapons • Electronic warfare • Adjust charging current [134]	• Directed energy includes jamming and spoofing techniques to manipulate the electromagnetic spectrum. Uplink jamming, aimed at satellites and space vehicles, can disrupt services for all users within the satellite's reception area. Spoofing introduces a false signal carrying incorrect information, deceiving the receiver. • Systems employing radio frequency jammers, lasers, chemical sprayers, or high-power microwaves can temporarily or permanently impair vehicles, causing potential damage.
V-TD9: Actuators	Body Control Module (BCM)	• Device control packet manipulation using fuzzing and sniffer. • Packet sniffing and targeted probing on a car • Access to CAN bus network • Practical attack [72,98,106,135] • Scalability is small	• The control of all vehicular body parts at motion, such as: – Continuous activation of Lock Relay – Activation of Windshield Wipers – Boot Unlocking – Unlocking doors – Permanent activation of horn – Disabling and enabling of headlights and auxiliary lights – Release of wiper fluid – Control of horn frequency – Control of instrument brightness – Physical access – Practical attack – Scalabililty is high

Table A6. *Cont.*

Trust Domain	Entry Point	Threat Description	Impact
V-TD9: Actuators	Electronic Control Module (ECM)	• Device Control Packet manipulation using fuzzing and sniffer. • Packet sniffing and targeted probing on a car • Access to CAN bus network [136,137] • Practical attack [72,98,106,110,135] • Scalability is small	• Initiate crankshaft or disturb engine timing by resetting the learned crankshaft angle through sensor errors • Temporary increase/boost idle RPM • Disable cylinders temporarily, power steering/brakes • Kill Engine • Disable the engine such that it knocks excessively when restarted, or cannot be restarted at all • Grind start
	Electronic Brake Control Module (EBCM)	• Device Control Packet manipulation using fuzzing and sniffer. • Packet sniffing and targeted probing on a car • Access to CAN bus network • Practical attack [72,98,106] • Scalability is small	• Lock of individual brakes without unlocking EBCM • Engages front left brake • Engages front right brake/Unlocks front Left • Unevenly Engages right brakes • Releases Brakes, prevents braking
	Autolock feature for doors, trunk, charging port and fuel lid—Passive key less entry system—Key fob [138]	• The Replay over the Cable attack involves relaying Low Frequency and Ultra High Frequency signals to activate the key fob and communicate with the vehicle. This is achieved using two antennas and an amplifier. The first antenna, located near the door handle, captures the beacon signal. This signal is then amplified and transmitted to the second antenna, which creates a magnetic field. The Passive Keyless Entry System (PKES) then demodulates this signal, enabling communication with the vehicle. • Remote access • Practical attack [72,96,98,106,139–152] • Scalability is high	• Passive Keyless Entry systems compromised • Vehicle unlocking • Ignition system
	Autolock doors and trunk-Passive key less entry system—Key fob [104]	• Replay over the air attack: RF link with emitter and receiver to receive, amplify, and transmit the signals from the car to the PKES. The emitter amplifies and transmits the vehicle's RF signals at 2.5 GHz. The vehicle's receiver gets the signal and converts it down to LF. Once the key fob reacts, the vehicle doors and even the engine can be unlocked. • Remote access • Practical attack • Scalability is high	• Passive keyless Entry systems compromised • Vehicle unlocking • Ignition system

Table A6. *Cont.*

Trust Domain	Entry Point	Threat Description	Impact
	• Cooperative Awareness Message (CAM) [116]	• Malicious advertisers (V2V/V2I) generate congestion response messages based on the content of the congestion requests [12,25,33,103] • Proximity—Remote access [116] • Simulated attack [116] • Scalability is high [116]	• The overall speed of CAVs could be affected. Increase in traffic in the targeted or neighbouring roads. Parked bot or compromised vehicles could be infected
V-TD10: Data Analysis	• Cooperative cruise control module • Localisation • Vehicle Control Warning, e.g., Lane Departure Warning • Vehicle Intersection Warning • Object Identification • Vehicle control automation • Sensor fusion	• Fake environmental conditions for camera lens [119] • Inject fabricated frames directly in camera processing and memory • Infect camera firmware in order to generate fabricated frames indicating unintentional activities such as lane departure • Frames are modified with property change such as blurry images to confuse modeling software • Insert fabricated frameworks and graphic models to indicate warnings • Remove frames that indicate normal or abnormal conditions • Deter/Rush/Delay delivery of speed, steering wheel info, status • Inject code that processes frames and generate models or alter internal memory with fabricated frames [12,25,33,103] • Inject code to fuse sensed data to indicate warnings and malicious outputs [99,119,129,153]	• Compromised cooperative cruise control functionalities leading to: – Lead to an accident – Inability to activate function – Lead to traffic – Lead to discomfort • The following are the subimpacts: – Sensor information altered – Sensor pre-processor manipulated – Main processor manipulated – Audio system exposed – HMI is vulnerable – Low level controllers influenced – Vehicle status altered – Road and environmental condition prediction module influenced – Altered video frames, graphic models – Altered vehicle dynamics information
V-TD11: Devices and Peripherals	• Bluetooth-enabled smartphone devices [104,154] • Company owned proprietary devices	• Indirect Bluetooth access: Vulnerability present in the custom interface code of the Bluetooth enabled telematics system. This requires pairing of an adversarial device to the vehicles Bluetooth • Direct Bluetooth access: Vulnerability present in the custom interface code of the Bluetooth enabled telematics system. This requires pairing of an adversarial device to the vehicles Bluetooth • Execution of any arbitrary code and taking control of the entire Vehicular systems • Remote access • Physical access [108] • Practical attack [97,107,144,155,156] • Scalability is small	• Execution of any arbitrary code and taking control of the entire vehicular systems by access to program handling Bluetooth functionality • Compromise of Telematics ECU's Unix operating system • Exfiltration of data
	• User devices (insider, guest, bring-your-own-device for employees) [104] • Mobile applications	• Information injection: device controlled by an adversary can inject malicious code or information [69] • Service manipulation: virtual machines could be manipulated • Information disclosure of vehicles and RSUs [117,134,142,157,158]	• Execution of any arbitrary code and taking control of the entire Vehicular systems by access to program handling Bluetooth functionality • Compromise of Telematics ECU's Unix operating system • Exfiltration of data

Table A7. Edge cloud and cloud threats.

Trust Domain	Entry Point	Threat Description	Impact
E-TD1, C-TD1 Edge/Cloud Communication (Wifi, Cellular, 5G/LTE)	Wireless Communication (Wifi, 5G/LTE)	• Denial of Service and distributed DoS by wireless jamming • Adversaries can launch attacks such as eavesdropping and/or traffic injection • Public network IP [94,105] • Rogue Gateway: Open system where any devices can part of the system	• Disrupt the vicinity of impacted network • Channel Hopping • Reactive jamming detection techniques, control channel attack prevention • Trigger node identification • Gateway compromised and access to internal network interfaces. Dangerous attack • An adversary may gain privileges to propagate network and create personal cloudlets
E-TD2, C-TD3: Microservices	Wireless communication, virtualisation servers	• Physical damage: The systems may not be guarded as they may be managed by service provider • Privacy leakage: Internal threats and honest but curious actors may attempt access the information [94,105] • Privilege escalation: Infrastructure could be misconfigured • Service Manipulation such as amending the functions of a CAV application, such as forming, join, leave, merge, split, end, and change leader. • Covert channel attack • Black/grey hole attack	• The impact of both the attacks are limited to the local vicinity and scope • The impact can be even worse as they can extract sensitive information about the users in the location due to contextual awareness
E-TD3, C-TD4: API	Local infrastructure interface, Vehicle-to-Car Interfaces	• Privacy leakage: Internal threats and honest but curious actors may attempt access the information [94,96,105,128] • Privilege escalation: Infrastructure could be misconfigured • Service Manipulation such as amending the functions of a CAV application [159] • Rogue Services	• The impact of both the attacks are limited to the local vicinity and scope • In some cases the distributed services and migrating virtual machines • The impact can be even worse as they can extract sensitive information about the users in the location due to contextual awareness
E-TD4, C-TD7: Physical Input/Outputs	Edge ports with devices and peripherals	• Direct Physical Access through connected devices • Practical attack • Scalability is small	• Disrupt the Edge • Inject false messages • Interrupt the functioning of edge • Exfiltrate data
E-TD5, C-TD2: Edge Process & Data Analysis	Wrong data, protocols and data from communication, microservices and data storage module [25,103]	• Inject Fake environmental conditions for edges [119] • Inject fabricated data directly in edge processing and memory • Infect firmware in order to generate fabricated data indicating unintentional activities such as lane departure • Frames are modified • Remove data that indicate normal or abnormal conditions • Deter/Rush/Delay delivery of data • Inject code that processes frames and generate models or alter internal memory with fabricated frames • Inject code to fuse sensed data to indicate warnings and malicious outputs [108,160,161]	• Mid-level vehicle function optimiser, Local Dynamic Map, Security Management, Edge Platform Management • The overall information for CAVs could be affected. Can lead to joint increase in traffic in the targeted or neighbouring roads. Parked bot or compromised vehicles could be infected • Lead to traffic • Lead to discomfort

Table A7. *Cont.*

Trust Domain	Entry Point	Threat Description	Impact
E-TD6, C-TD5: Data Storage	• Firmware • Firmware Update • Debug info. • Local Dynamic Map • System level information • Software	• Inject fabricated frames in memory, e.g., blurry frames, wrong tags • Amend firmware to produce fabricated frames leading to creation and deletion of point cloud or frames • Deter/accelerate/delay status and information of modules • Inject malicious coordinates to places • Remote access with/without cables for information loss [157,162,163] • Replay of frames • Delete/reveal the system software or data [105] • Proximity— Remote access [116] • Simulated attack [116,164–171] • Scalability is high [116]	• False warnings or services • Removed warnings or services • Delayed warnings or services
E-TD7, CTD8: Energy System	Energy and Fuel Storage, Power Generation	• Energy and Fuel Storage, Power Generation, and Directed Energy Weapons • Electronic Warfare • Kinetic Energy Threats	• Directed Energy is able to operate as a force multiplier without visual signs or detection. As a result, it can ultimately damage the targeted unit and cause losses. • It includes jamming and spoofing to control the electromagnetic spectrum. Uplink jamming can be directed toward the satellite and space orbiting vehicles, which can impair the services for all users in the satellite reception area. Spoofing deceives the receiver by introducing a fake signal with erroneous information.
E-TD8: Actuators	Edge processing and physical access	• Manipulate actuators • Disable actuators	• The Control of all edge based actors: • Manipulate or disable barriers • Manipulate or disable traffic signal
E-TD9, C-TD6: Monitoring	White box and black box attack	• Adversarial model is more effective at producing successful mispredictions of signboards at a quicker pace and with a larger likelihood of failure [133] • Remote access • Theoretical attack • Scalability is high	• Mispredictions of signboards
E-TD10: Edge Sensors	Internal sensors which relies on the network layer [172]	• Jamming attack • Timing attack • Replay attack • Routing threats	• Uniform coding • Conflict collision • Privacy disclosure • Redundant sensors with integrity checks • Sensor Fusion • Attack detection techniques • Noise Filters • Machine learning based solutions
	External sensors include rain sensors, pH sensors, smart meters, temperature sensors, humidity sensors, sound sensors, vibration sensors, chemical sensors, pressure sensors [172]	• Tampering • Sensor device capture • Fake device and malicious data • Sybil attack • Source device authentication problem • Implicit deduction from sensor behaviour • Encryption leakage	

Table A7. *Cont.*

Trust Domain	Entry Point	Threat Description	Impact
E-TD11: Devices	User devices (insider, guest, bring-your-own-device for employees) [104]	• Information injection: device controlled by an adversary can inject malicious code or information [69] • Service manipulation: virtual machines could be manipulated • Information disclosure of vehicles and RSUs [158,162]	• Execution of any arbitrary code and taking control of the entire Vehicular systems by access to program handling Bluetooth functionality • Compromise of Telematics ECU's Unix operating system • Exfiltration of data
E-TD12: Roadside Infrastructure	These devices could be end-notes such as COHDA units or internet-of-things devices	• Wired connections could be manipulated to connect with rogue systems to give feedback to edge systems with artificially coded messages • Execution of any arbitrary code and taking control of the RSUs • Remote access • Practical attack [108,155,156,160,161,173,174] • Scalability is high	• Execution of any arbitrary code and taking control the systems by access to programs • Compromise of operating system • Exfiltration of data • Analysis of the current contextual awareness

Table A8. Incidents from practical attacks classified based on Real Life—Incident Code (RL-IC), trust domain (TD), news date, incident title, and threat description.

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC0 [162]	E-TD6, E-TD11, C-TD5	08-Aug-11	First remote hack of a vehicle, gaining control of a Chevy Malibu was established	• First-ever real-life demonstration of car hack • Full control of car using Bluetooth
RL-IC1 [162]	E-TD6, E-TD11, C-TD5	26-Jun-15	Information on 100,000 Citroen owners may have been leaked	• Hacker selling car owner data • Database screenshot revealed orders, personal information • Importance of car data security highlighted
RL-IC2 [72]	V-TD1, V-TD9	21-Jul-15	Jeep and Chrysler can be remotely hijacked, Chrysler recalls 1.4 million cars and trucks	• 1.4 million cars and trucks recalled by Chrysler • recall prompted by demonstration of remote hacking • hackers able to access key functions of the vehicle
RL-IC3 [97,175]	V-TD1, V-TD11, V-TD9	30-Jul-15	GM's Onstar system has a security flaw	• Vulnerability in OnStar system revealed by researcher Samy Kamkar • Device named OwnStar can track and unlock OnStar equipped vehicles remotely • Highlights security risks in connected car systems
RL-IC4 [139]	V-TD9	25-Dec-15	Volvo, BYD, Buick Regal door lock remote control rolling code mechanism is bypassed	• Ghost Ax Lab found design flaws in anti-theft systems of some Volvo, BYD, and Buick vehicles • Flaws in HCS rolling code chip and Keeloq algorithm • Ghost Ax Lab can reproduce car remote control key function • Unlimited reproduction of car remote control key breaks security systems • Manufacturer recall needed, difficult for users to prevent

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC5 [159]	E-TD3, C-TD4	24-Feb-16	Controlling vehicle features of Nissan Leafs across the globe via vulnerable APIs	• The post will delve further into the details of the risk and what it enables someone to do • An attendee at a workshop discovered that he could control Nissan LEAF vehicles over the internet, including not just their own but also those of other people • The attendee, along with fellow security researcher Scott Helme, recorded a video to demonstrate the issue • The post will delve further into the details of the risk and what it enables someone to do
RL-IC6 [105]	C-TD1,V-TD2, C-TD4, C-TD3, C-TD5	06-Mar-16	C4max TGU is improperly configured and exposed to the public network	• New Eagle TGU can be accessed without auth via public IP/Telnet port 23 • Telnet allows access to GPS, network, speed, voltage, alarms, etc. • Can set area restrictions, control CAN bus and other features.
RL-IC7 [98]	V-TD1, V-TD9	05-Jun-16	Pen test partners controls Mitsubishi Outlander with Wi-Fi	• C4Max Telematics Gateway Unit (TGU) manufactured by New Eagle can be accessed without authentication • Through Telnet, vehicle's GPS route, modem network, speed, battery voltage, alarms, and other information can be obtained • Telnet also allows setting up area restrictions on vehicles and control of CAN bus
RL-IC8 [106]	V-TD9, V-TD3, V-TD2	08-Aug-16	Mirrorlink buffer overflow vulnerability	• MirrorLink vulnerability discovered by NYU and George Mason researchers • Standard jointly established by mobile phone and car manufacturers • Vulnerability allows hackers to take control of critical safety components in the vehicle.
RL-IC9 [158]	E-TD11, V-TD11	25-Apr-17	Hyundai blue link phone app information leaked	• Hyundai Blue Link mobile app leaks sensitive user and vehicle information • Vulnerability in new log upload function • Attacker can obtain car owner's personal information via man-in-the-middle attack.
RL-IC10 [107]	V-TD2, V-TD11	23-May-17	BMW 330i 2011 format string DoS vulnerability (CVE-2017-9212)	• BMW 330i connects to Bluetooth with a format string (%c or %x) • Causes multimedia software to crash
RL-IC11 [108]	V-TD7, V-TD2-D, V-TD11, E-TD12, E-TD5	27-Jul-17	Vulnerabilities in Ford, BMW, Infiniti, and Nissan TCUs can be hacked remotely	• Researchers from McAfee discovered vulnerabilities in TCU (2G modem) used in cars • Vulnerabilities affect the S-Gold 2 cellular baseband chip • One vulnerability requires physical access but the other can be exploited remotely
RL-IC12 [99]	V-TD2, V-TD1, V-TD10, V-TD9	30-Apr-18	Volkswagen, Audi in-vehicle entertainment system vulnerabilities	• Researchers discovered security flaws in VW and Audi vehicles • Attacker can launch remote attack and control RCC and CAN bus • Vulnerability in Volkswagen's in-vehicle infotainment system can be exploited remotely, giving attacker access to manipulate car's braking and steering systems

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC13 [140]	V-TD9	10-Sep-18	Hackers can copy keys to steal Tesla model s in seconds (CVE-2018-16806)	• Researchers discovered security issue in Tesla Model S PKES and wireless key • Hackers can copy the car key and steal the car • Vulnerability in the authentication process allows hackers to obtain the car's identity information and exploit the weak two-way authentication and small key space
RL-IC14 [156]	V-TD11, E-TD12	14-Oct-18	An online car-hailing driver was jailed for stealing electricity 382 times in half a year using the pinch gun method and card second method	• Dong Mou, a car-hailing driver in Beijing, used loopholes in State Grid charging software to steal electricity using the pinch gun method and card second method • He stole electricity 382 times, charged with theft and teaching criminal methods • Sentenced to 1 year in prison and fined 1000 CNY
RL-IC15 [115]	V-TD3, V-TD5	28-Nov-18	FHI Subaru Starlink Harman local update verification flaw (CVE-2018-18203)	• Vulnerabilities in Subaru StarLink vehicles update mechanism • Attackers can flash tampered firmware via USB • Attackers can execute arbitrary code with root privileges.
RL-IC16 [134]	V-TD8, V-TD11	13-Dec-18	Chargepoint's home chargers have multiple vulnerabilities	• Kaspersky discovered vulnerabilities in ChargePoint's home charging piles • Remote attackers can adjust charging current and stop charging process • Vulnerabilities in device's web server pose potential physical and economic damage
RL-IC17 [141]	V-TD9	03-May-19	Ford key vulnerability replay attack	• Vulnerabilities found in Ford's wireless key fobs • Attacker can unlock doors and start engine using a device costing 300 USD • Attacker captures and replays rolling code signal, control of vehicle possible
RL-IC18 [109]	V-TD4	19-Jun-19	Tesla model 3 GPS spoofing	• Regulus Cyber tests on Tesla's GPS system show it can be hacked using off-the-shelf tools in under a minute • Hack causes extreme driving instability and incorrect signals, lane changes, and exits • Hack exposes the risk of deviation when relying solely on GPS signal, requires other data for correction
RL-IC19 [163]	V-TD2, V-TD3	14-Jul-19	10,000 USD XSS vulnerability in Tesla	• White hat hacker Sam Curry found cross-site scripting (XSS) vulnerability on Tesla cars • Vulnerability allows unauthorised access to vehicle information, such as VIN, speed, temperature, lock status, tire pressure, alarm, and time zone • Curry used the XSS Hunter attack payload to test the vulnerability, which was triggered by maintenance staff in the vehicle name field
RL-IC20 [127]	C-TD5	31-Jul-19	Honda leaks 40 GB of internal data due to improper database configuration	• Honda Motor misconfigured an ElasticSearch database • Database containing 134 million documents of employee information (40 GB) of data leaked

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC21 [157]	V-TD11, C-TD5	19-Oct-19	Mercedes-Benz app can see other car owners' information in the US' explosion security breach	• Security breach in Mercedes-Benz app in the US • Personal information of other car owners exposed • Reports of app incorrectly displaying account and vehicle information of other owners, including names, recent events, phone numbers
RL-IC22 [142]	V-TD11, V-TD9	14-Nov-19	Tesla iBeacon privacy leak	• Bluetooth security expert Martin Herfurt discovered that Tesla Model 3 vehicles continuously broadcast a set of unique ID numbers (iBeacon) through Bluetooth. • These ID numbers are used as a parameter for the mobile app to open and close the car doors, but cannot be changed or turned off by the user, creating a potential privacy concern. • Herfurt created an app and global Tesla monitoring platform to track the use of these ID numbers.
RL-IC23 [100]	V-TD1, V-TD3	02-Jan-20	Exploitation of Marvell wireless protocol stack vulnerabilities on Tesla Model S	• Tencent Keen Lab found two vulnerabilities in the wireless function module of a Model S vehicle • The vulnerabilities exist in the firmware and driver of the Marvell 88W8688 chip • An attacker can use these vulnerabilities to execute arbitrary commands in the Linux system of the module.
RL-IC24 [119]	V-TD10	19-Feb-20	Using machine learning to adversarially attack Telsa and Mobileye's ADAS	• McAfee researchers used adversarial machine learning to manipulate Tesla's Autopilot system, Mobileye EyeQ 3 • This system was fooled by a subtle change in a speed limit sign • The change caused the Tesla to speed in a lower speed zone.
RL-IC25 [164]	V-TD7, V-TD9	23-Mar-20	Tesla model 3 central control denial of service vulnerability (CVE-2020-10558)	• Tesla Model 3 has a security vulnerability in the Driving Interface version before 2020.4.10 • Vulnerability is caused by program not properly isolating process • Attacker can exploit vulnerability by tricking car owner into visiting malicious web page, resulting in crashing of central control dashboard system functions
RL-IC26 [110]	V-TD9, V-TD2	30-Mar-20	Tencent keen lab: Lexus car safety research summary report	• Researchers at Keen Lab found security issues in the Bluetooth and vehicle diagnostic functions of a 2017 Lexus NX300 model. • These issues can endanger the AVN system, in-car CAN network, and related electronic control units. • By exploiting these issues, the researchers were able to remotely control the AVN system and send malicious commands to the car's CAN network, potentially causing unexpected physical actions
RL-IC27 [135]	C-TD5	18-May-20	Mercedes-Benz on-board logic unit (OLU) source code leaked	• Daimler failed to properly implement account verification process • Researchers were able to register with non-existent corporate email and download 580 Git repositories • Leaked projects include source code for Mercedes-Benz OLU components, internal Daimler components, and more.

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC28 [155]	E-TD12, V-TD11	28-May-20	CVE-2020-12493: traffic lights exposed serious loopholes, which can be manipulated to cause traffic paralysis	• Signal light controller manufacturer SWARCO has a vulnerability that allows hackers to destroy traffic lights and manipulate them at will. • The vulnerability was discovered by German industrial network security consulting company ProtectEM during a security audit of a German city. • The vulnerability is an improper access control vulnerability that allows hackers to gain root access to the device without permission. It was reported to SWARCO in July 2019 and a patch was provided to customers in April 2020.
RL-IC29 [94]	V-TD1, V-TD2, E-TD1, E-TD2, E-TD3	20-Jul-20	360 Sky-Go team releases Mercedes-Benz security research report: 19 vulnerabilities, work together to fix	• The 360 Sky-Go team conducted a year-long information security study on Mercedes-Benz • They identified 19 security vulnerabilities in various networking modules including the head-unit, vehicle communication module, and Internet of Vehicles communication system • These vulnerabilities are expected to affect over 2 million Mercedes-Benz cars in China
RL-IC30 [130]	V-TD4	23-Jul-20	Tesla NFC relay attack (CVE-2020-15912)	• Kevin and team Tiger conducted research and testing on Tesla NFC key. • Successful relay attack on Tesla Model 3's NFC keys trough Wi-Fi, opening the door.
RL-IC31 [173]	E-TD12	24-Oct-20	There are serious security loopholes in non-inductive payment charging piles, and there are hidden dangers of stealing brushes	• Blade Team from Tencent successfully demonstrate attack on 'non-inductive payment' DC charging pile • They connected with the charging pile with car by stimulating victim's ID compromising authentication
RL-IC32 [111]	V-TD2, V-TD3	10-Nov-20	CVE-2020-28656: VW Polo local upgrade check bypass	• VW polo 2019 infotainment system has flaw • Attackers could execute arbitrary code through physical contact with root privileges
RL-IC33 [117]	V-TD9, V-TD11, V-TD3	23-Nov-20	Tesla Model X bluetooth key vulnerability	• Lennert Wouters found Tesla Model X keyless entry system lacks firmware update check • Attacker could rewrite the firmware of the key fob through Bluetooth connection • The car could be unlocked within few minutes
RL-IC34 [143]	V-TD2, V-TD9	28-Apr-21	Two white-hat hackers 'hacked' Tesla with drones	• Tesla's doors and trunk unlocked using zero-click vulnerabilities through drones • Attackers hacked infotainment system through WiFi
RL-IC35 [79]	V-TD2	21-May-21	Tencent keen lab: Mercedes-Benz car information security research summary report	• Keen lab found vulnerabilities in Mercedes-Benz's infotainment system MBUX • Head Unit and T-Box were the attack surface used for successful demonstration.

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC36 [144]	V-TD9, V-TD11	04-Jun-21	Canadian programmers discover Bluetooth key vulnerability that allows anyone to unlock a Tesla	• Shankar Gomare found vulnerability in Voice for Tesla's unlocking • Flaw in Bluetooth connections to vehicles without authentication • Strongest Bluetooth for connected device within range receives unlock signal
RL-IC37 [165]	C-TD5	11-Jun-21	Data of 3.3 million Volkswagen customers leaked	• 3.3 million Volkswagen group's customer data exposed by a vendor unprotected on the internet • Sensitive data including loan qualification and social security numbers were also leaked • Affected region include the US and Canada
RL-IC38 [166]	C-TD5	24-Jun-21	The data of nearly 1000 Mercedes-Benz users were leaked, including driver's license and credit card information	• Sensitive personal information of Mercedes-Benz customers and interested buyers leaked on cloud storage platform • Mercedes-Benz evaluated 1.6 million customer records to determine the impact • Data breach exposed less than 1000 customer's credit card and social security number for potential buyers
RL-IC39 [160]	E-TD12, E-TD5	13-Jul-21	Schneider charging pile vulnerability	• BaCde and Kevin2600 acquired remote Root shell of Schneider charging piles without user interaction • Two high-risk vulnerabilities, CVE-2021-22707 and CVE-2021-22708, were discovered
RL-IC40 [145]	V-TD9	04-Aug-21	Honda Accord, Civic, Acura, and other vehicles have wireless key replay attack vulnerabilities	• Keys of Honda Accord, Acura, and Civic use unsafe fixed code, vulnerable to replay attack • Attacker could unlock doors, trunks, and control windows.
RL-IC41 [153]	V-TD10	17-Aug-21	QNX is affected by the Badalloc vulnerability	• Blackberry's QNX real-time operating system (RTOS) allows attacks to damage and control automobiles, medical devices, and industrial equipment • Car manufacturers including BMW, Audi, and VW use this. In total, 195 million vehicles use this system globally • Attacker could exploit memory allocation functions to perform heap overflow, resulting in malicious code execution
RL-IC42 [95]	V-TD1	22-Sep-21	The man blocked with a melon seed bag and evaded fees 22 times worth over 40,000 CNY in 3 months	• Expressway tolls evaded 22 times using melon seed bags to shield ETC and CPC signals • Actual trajectory of the vehicle remains unrecognised to billing system • Evaded fees total 40,000 CNY
RL-IC43 [167]	C-TD5	20-Dec-21	Volvo cars reveals security breach that led to R&D data being stolen	• File repository illegally accessed by third Party • Attack claimed by 'Snatch Ransomware gang' using screenshot as evidence • Volvo cars stocks in Stockholm fall 3.5%

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC44 [146]	V-TD9	31-Dec-21	There is a defect in the rolling code of the Honda car key, and the wireless signal can be replayed (CVE-2021-46145)	• Design flaw found in Honda car key by Qi Anxon Xingyu Lab and Kevin2600 • Attacker could open the door by rolling back the synchronisation counter using expired door opening instructions
RL-IC45 [168]	C-TD5	01-Mar-22	Supplier hit by cyber attack, Toyota shuts all factories in Japan for one day	• On February 26, Toyota's supplier Kojima Press Industry discovered an error on a file server with a threatening message • Incident caused all Toyota's factories in Japan to shutdown, affecting production of about 13,000 vehicles
RL-IC46 [147]	V-TD9	13-Mar-22	Replay vulnerability in Tesla charging cover (CVE-2022-27948)	• Wireless signal used to open Tesla charging port cover uses a fixed code • Attacker can replay the wireless signal and open the charging port cover anywhere • Dedicated wireless key for unlocking the charging port cover sold
RL-IC47 [169]	C-TD5	14-Mar-22	Denso German branch was attacked by cyber attack and 1.4tb of data were stolen	• Unauthorised malware access detected in Denso's Grmany sales and engineering branch • A group called Pandora threatened to disclose commercial secrets on the dark web • 1.4 TB of data including 157 k purchase orders and sketches were claimed to be obtained • Ransom was demanded by the hacker to prevent leakage on the dark web
RL-IC48 [148]	V-TD9	25-Mar-22	Honda car keyless entry system replay attack (CVE-2022-27254)	• Wireless keys of some Honda and Acura are not encrypted and used fixed codes • Attacker could open the door and remotely start the car's engine using replay attack
RL-IC49 [161]	E-TD12, E-TD5	29-Apr-22	Xingyu lab discloses a variety of charging pile vulnerabilities	• Independent IPs of charging piles exposed on public network • Multiple vulnerabilities including exposure of account number and password of the system, lack of access control, and unauthorised command injection were found • This was due to use of hardcoding in the firmware
RL-IC50 [149]	V-TD9	15-May-22	Tesla Model3/Y Bluetooth relay attack	• Keyless entry system of Tesla Modle 3 and Y can be compromised using Bluetooth link layer data, disclosed by the NCC • Attacker could unlock the car and start the engine • The whole process only takes 10 s to complete.
RL-IC51 [150]	V-TD9	09-Jun-22	Create any Tesla bluetooth key	• Method to register new Tesla's key revealed by Martin Herfurt of Trifinite • Attacker could create new key within 130 s of door unlocking using NFC key, compromising door locks
RL-IC52 [112]	V-TD2	12-Jun-22	Hyundai/Kia local upgrades cracked	• Engineer Daniel Feldman cracked the infotainment system of their car • Private key obtained was found over google revealing encrypted files in ZIP archive of Hyundai's firmware

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC53 [151]	V-TD9	07-Jul-22	Rolling pawn: wireless key rolling code rollback vulnerability	• Design flaw found in Honda wireless (RF) key by Kevin2600 and Wesley Li • Sending continuous car control commands would cause rolling code counter to roll back • Attacker could open the door and start the engine
RL-IC54 [128]	C-TD4, V-TD4	19-Jul-22	Micodus vehicle tracker security vulnerability affects over a million cars worldwide	• Advisory warning issued by U.S. Cybersecurity and Infrastructure Security Agency (CISA) on multiple security vulnerabilities on MiCODUS MV720 GPS tracking system • More than 1.5 million vehicles could be affected • Attackers could track vehicle in real time, access historical routes, and cut off engine of a driving vehicle
RL-IC55 [113]	V-TD4, V-TD7	23-Aug-22	Some brands of cars in Shanghai display screen prompts "there is a gunfight on the road?"	• Traffic warning message Gunfight on the road was relayed on car display • Porsche and Audi car owners in Shanghai were affected • Industry believe this could be a translation problem; however, the possibility of hacking cannot be ruled out
RL-IC56 [129]	V-TD4, V-TD10	01-Sep-22	Yandex taxi was manipulated by hackers, and there was a traffic jam in Moscow	• A vulnerability was discovered in the mailbox system of Hyundai and Genesis user registration that allows authorised users to remotely control vehicles • The vulnerability is due to the fact that the email addresses used for authentication were not properly verified • By using a specific technique (CRLF), attackers can deceive the system and take over the accounts of other users
RL-IC57 [170]	C-TD5	02-Oct-22	6.99 GB of internal files leaked from Italian supercar maker Ferrari	• 6.99 GB of Ferrari internal files were exposed on the dark web by a ransomware organisation, RandomEXX • Ferrari confirmed the authenticity of the documents, however no evidence of cyber attack was found • Production and operations were not affected
RL-IC58 [96]	V-TD9, V-TD1	30-Nov-22	Internet of vehicles service provider Sirius XM API vulnerability, unauthorised remote control of Honda, Nissan, Infiniti, and Acura cars	• Remote car control service of Sirius XM has Insecure Direct Object Reference vulnerability exposing remote control Token based on VIN code • Attacker could unlock the car, start the engine and obtain personal information of the car owner • Honda, Nissan, Infiniti, and Acura's cars were affected
RL-IC59 [96]	E-TD3, C-TD4	30-Nov-22	Hyundai, Genesis auto account hijacking	• A vulnerability was discovered in the mailbox system of Hyundai and Genesis user registration that allows authorised users to remotely control vehicles • The vulnerability is due to the fact that the email addresses used for authentication were not properly verified • By using a specific technique (CRLF), attackers can deceive the system and take over the accounts of other users

Table A8. *Cont.*

Real Life Incidents				
RL-IC	**TD**	**Date**	**Incident Title**	**Threat Description**
RL-IC60 [174]	E-TD12	07-Dec-22	Replay attack: numerous traffic lights in Germany are vulnerable to manipulation	• Security researchers demonstrate traffic light system manipulation using unencrypted radio signals • Attacker could artificially extend traffic lights creating traffic jams or confusion • The risk is considered to be low
RL-IC61 [101]	V-TD1, V-TD2, V-TD3	07-Dec-22	Multiple vulnerabilities disclosed in Black Hat Europe VW iD series	• Security researchers from NavInfo Europe BV discover Volkswagen ID series is vulnerable to arbitary code execution on the QNX7 network service • Attacker could extract secret keys intrusted zones of gateways and remote access via Wi-Fi to install backdoors • Infotainment system GUEST OS local USB upgrade does not verify the shell in the U disk
RL-IC62 [171]	C-TD5	20-Dec-22	Nio data leaked and blackmailed	• 22.8 k NIO internal employee data and 399 k ID card data of car owners and users were leaked by a cyber criminal • 2.25 million USD was extorted in bitcoins • NIO's Weilai apologised publically for the impact on users and promised to take responsibility for the losses caused due to this incident
RL-IC63 [152]	V-TD9	31-Dec-22	Luxury cars are gone in 90 s with thief kit	• Device using Bluetooth speakers and old mobile phones to unlock and start luxury cars found being sold online for 1300 GBP • Attackers could steal the cars from driveways in 90 s using this

Table A9. Attack vector description.

Attack Vector			
Attack Level 1	**Attack Level 2**	**Attack Level 3**	**Description**
Manipulate System Resources	Infrastructructure Manipulation	Black Hole Attack [65]	In a platooning context, a black hole attack involves a malicious vehicle falsely advertising itself as having the shortest path to the destination. This leads other vehicles to send data through it, but the malicious vehicle drops all the packets, disrupting communication and coordination. This attack can cause significant disruptions in platooning operations, including loss of critical data and misguiding the platoon about route and safety-related information. It undermines the integrity and availability of the platooning system, posing risks to both operational efficiency and vehicle safety.
Engage in deceptive intersections	Identity spoofing	Sybil Attack [176]	A Sybil attack involves a single malicious vehicle creating multiple fake identities to gain a disproportionate influence in the platooning network. This can lead to manipulation of collective platooning decisions, such as route selection or speed adjustments, and can disrupt the normal operation of the platoon. The attack undermines the trust and authenticity within the platooning system, posing significant challenges to its coordination and safety mechanisms.
Subvert access control	Exploiting trust in client	Man-In-the-Middle [177]	In this attack, an attacker intercepts and potentially alters the communication between two platooning vehicles without their knowledge. This can result in the leakage of sensitive information or introduction of false commands. It can severely impact the decision-making process in platooning, as altered commands or data can lead to incorrect manoeuvres, increasing the risk of collisions or inefficient routing. This attack compromises the confidentiality and integrity of the platoon's communication, leading to potential operational and safety hazards.
Abuse existing functionality	Flooding	Flooding attack [178]	A flooding attack in a platooning system involves overwhelming the network with excessive traffic, which can lead to delays or blocking of legitimate communication among the vehicles. This could result in reduced responsiveness of the platoon to dynamic traffic conditions, increasing the risk of accidents and reducing operational efficiency. The attack primarily affects the availability of the platoon network, leading to potential communication and coordination failures.

Table A9. *Cont.*

Attack Vector			
Attack Level 1	**Attack Level 2**	**Attack Level 3**	**Description**
Inject unexpected items	Traffic injection	Message Injection attack [179]	In a platooning scenario, a Message Injection Attack involves an attacker inserting false or malicious data into the communication stream of the platoon. This could be false sensor readings, misleading location data, or incorrect routing information. The injected false data can lead to misguided decisions by the platooning vehicles, such as incorrect route adjustments, speed changes, or even evasive manoeuvres, potentially causing disarray in the platoon formation and increasing the risk of accidents. This type of attack targets the integrity and authenticity of the data being shared within the platoon, severely compromising the reliability and safety of the platooning operations.
Collect and analyse information	Interception	Eavesdropping [180]	In platooning, an Eavesdropping Attack involves unauthorised interception of communications between vehicles. This could be capturing vehicle status data, platoon formation details, or sensitive operational information. This attack can compromise the confidentiality of the platoon's communications, leading to potential misuse of sensitive data. It could also facilitate further attacks by providing crucial insights into the platoon's operations and vulnerabilities. The major risk here is the breach of privacy and security, as sensitive data can be exploited to manipulate or disrupt platooning operations, or even for malicious purposes outside the immediate context of platooning.
Employ probabilistic techniques	Employ probabilistic techniques	packet fuzzing [181]	In platooning microservices, a Packet Fuzzing Attack involves sending malformed or random data packets to the network or vehicles within the platoon. The goal is to test the robustness of the system and identify vulnerabilities that can be exploited. This type of attack can lead to various issues, such as triggering unexpected behavior in vehicle control systems, causing communication disruptions, or even crashing systems if they are not properly handling malformed data. The primary risks of packet fuzzing attacks in a platooning context are the potential to uncover and exploit security vulnerabilities, leading to operational disruptions or safety hazards. Effective handling and validation of data packets are essential to mitigate these risks.

Table A9. *Cont.*

Attack Vector			
Attack Level 1	**Attack Level 2**	**Attack Level 3**	**Description**
Manipulate timing and state	Manipulate timing and state	Timing Attack [182]	In the context of platooning, a Timing Attack could involve analyzing the time taken by processes or communications to extract sensitive information or to infer internal states of the platoon's control systems. This type of attack could be used to subtly disrupt or manipulate the coordination and timing of platoon operations, such as altering the response times of vehicles to commands. It poses a risk to the reliability and predictability of platoon behaviors, potentially leading to inefficiencies or safety hazards. Session Hijacking in a platooning context involves an attacker taking over a vehicle's session after it has been authenticated within the platoon. This allows the attacker to gain unauthorised control over the vehicle's operations within the platoon. This could result in the hijacked vehicle exhibiting unexpected or dangerous behaviors, such as deviating from the planned route or making sudden manoeuvres, potentially leading to disorganisation or accidents within the platoon. The attack mainly compromises the session management of the platooning system, affecting its authenticity and authorisation mechanisms, thereby posing a threat to the operational security and safety of the platoon.

References

1. Granovskii, M.; Dincer, I.; Rosen, M.A. Economic and environmental comparison of conventional, hybrid, electric and hydrogen fuel cell vehicles. *J. Power Sources* **2006**, *159*, 1186–1193. [CrossRef]
2. NHTSA. *Federal Automated Vehicles Policy*; U.S. Department of Transportation, NHTSA: Washington, DC, USA, 2016.
3. Foxx, A.R. *Beyond Traffic: 2045 Final Report*; Department of Transportation: Washington, DC, USA, 2017.
4. Miller, C.; Valasek, V. Remote Exploitation of an Unaltered Passenger Vehicle. *Black Hat USA* **2015**, *2015*, 13–85.
5. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
6. Salek, M.S.; Khan, S.M.; Rahman, M.; Deng, H.W.; Islam, M.; Khan, Z.; Chowdhury, M.; Shue, M. A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. *IEEE Internet Things J.* **2022**, *9*, 8250–8268. [CrossRef]
7. NHTSA. Vehicle Cybersecurity. Available online: https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity (accessed on 20 August 2023).
8. Ge, X.; Han, Q.L.; Wang, J.; Zhang, X.M. Scalable and resilient platooning control of cooperative automated vehicles. *IEEE Trans. Veh. Technol.* **2022**, *71*, 3595–3608. [CrossRef]
9. Montanaro, U.; Dixit, S.; Fallah, S.; Dianati, M.; Stevens, A.; Oxtoby, D.; Mouzakitis, A. Towards connected autonomous driving: Review of use-cases. *Veh. Syst. Dyn.* **2019**, *57*, 779–814. [CrossRef]
10. Jia, D.; Lu, K.; Wang, J.; Zhang, X.; Shen, X. A survey on platoon-based vehicular cyber-physical systems. *IEEE Commun. Surv. Tutorials* **2015**, *18*, 263–284. [CrossRef]
11. Amoozadeh, M.; Deng, H.; Chuah, C.N.; Zhang, H.M.; Ghosal, D. Platoon management with cooperative adaptive cruise control enabled by VANET. *Veh. Commun.* **2015**, *2*, 110–123. [CrossRef]
12. Vasconcelos Filho, Ê.; Severino, R.; Salgueiro dos Santos, P.M.; Koubaa, A.; Tovar, E. Cooperative vehicular platooning: A multi-dimensional survey towards enhanced safety, security and validation. *Cyber-Phys. Syst.* **2023**, *9*, 1–53. [CrossRef]
13. Mousavinejad, E.; Yang, F.; Han, Q.L.; Ge, X.; Vlacic, L. Distributed cyber attacks detection and recovery mechanism for vehicle platooning. *IEEE Trans. Intell. Transp. Syst.* **2019**, *21*, 3821–3834. [CrossRef]
14. CAPEC. Common Attack Pattern Enumeration and Classification. Available online: https://capec.mitre.org/data/definitions/1000.html (accessed on 20 August 2023).
15. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [CrossRef]
16. Petit, J.; Shladover, S.E. Potential Cyberattacks on Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 546–566. [CrossRef]
17. Hamida, E.; Noura, H.; Znaidi, W. Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics* **2015**, *4*, 380–423. [CrossRef]
18. Sakiz, F.; Sen, S. A survey of attacks and detection mechanisms on intelligent trasnportation system—VANETS and IoV. *Ad Hoc Netw.* **2017**, *61*, 33–50. [CrossRef]
19. Parkinson, S.; Ward, P.; Wilson, K.; Miller, J. Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2898–2915. [CrossRef]
20. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]
21. Studnia, I.; Nicomette, V.; Alata, E.; Deswarte, Y.; Kaâniche, M.; Laarouchi, Y. Survey on security threats and protection mechanisms in embedded automotive networks. In Proceedings of the 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W), Budapest, Hungary, 24–27 June 2013; pp. 1–12.
22. Thing, V.L.L.; Wu, J. Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. In Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, China, 15–18 December 2016.
23. Al-Kahtani, M.S. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In Proceedings of the Survey on Security Attacks in Vehicular Ad Hoc Networks (VANETs), Gold Coast, Australia, 12–14 December 2012; pp. 1–9.
24. Gillani, S.; Shahzad, F.; Qayyum, A.; Mehmood, R. A survey on security in vehicular ad hoc networks. In *Proceedings of the Communication Technologies for Vehicles: 5th International Workshop, Nets4Cars/Nets4Trains 2013, Villeneuve d'Ascq, France, 14–15 May 2013*; Proceedings 5; Springer: Cham, Switzerland, 2013; pp. 59–74.
25. Othmane, L.B.; Weffers, H.; Mohamad, M.M.; Wolf, M. A survey of security and privacy in connected vehicles. In *Wireless Sensor and Mobile Ad-Hoc Networks Vehicular and Space Applications*; Springer: New York, NY, USA, 2015; pp. 217–247.
26. Yan, G.; Wen, D.; Olariu, S.; Weigle, M.C. Security challenges in vehicular cloud computing. *IEEE Trans. Intell. Transp. Syst.* **2013**, *14*, 284–294. [CrossRef]
27. Engoulou, R.G.; Bellaiche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
28. Siegel, J.E.; Erb, D.C.; Sarma, S.E. A Survey of the Connected Vehicle Landscape Architectures, Enabling Technologies, Applications, and Development Areas. *IEEE Trans. Intell. Transp. Syst.* **2017**, *99*, 2391–2406. [CrossRef]
29. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]

30. Boumiza, S.; Braham, R. Intrusion threats and security solutions for autonomous vehicle networks. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, 30 October–3 November 2017; pp. 120–127.
31. Kelarestaghi, K.B.; Foruhandeh, M.; Heaslip, K.; Gerdes, R. Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures. *arXiv* **2019**, arXiv:1903.01541.
32. Sheikh, M.S.; Liang, J. A comprehensive survey on VANET security services in traffic management system. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 2423915. [CrossRef]
33. Sommer, F.; Dürrwang, J.; Kriesten, R. Survey and classification of automotive security attacks. *Information* **2019**, *10*, 148. [CrossRef]
34. Jadhav, S.; Kshirsagar, D. A survey on security in automotive networks. In Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16–18 August 2018; pp. 1–6.
35. Yoshizawa, T.; Preneel, B. Survey of security aspect of v2x standards and related issues. In Proceedings of the 2019 IEEE Conference on Standards for Communications and Networking (CSCN), Granada, Spain, 28–30 October 2019; pp. 1–5.
36. Masood, A.; Lakew, D.S.; Cho, S. Security and privacy challenges in connected vehicular cloud computing. *IEEE Commun. Surv. Tutorials* **2020**, *22*, 2725–2764. [CrossRef]
37. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Commun. Surv. Tutorials* **2021**, *23*, 6240–6259. [CrossRef]
38. Zeadally, S.; Hunt, R.; Chen, Y.S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [CrossRef]
39. Di Pietro, R.; Guarino, S.; Verde, N.V.; Domingo-Ferrer, J. Security in wireless ad-hoc networks–a survey. *Comput. Commun.* **2014**, *51*, 1–20. [CrossRef]
40. ETSI. Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. *Eur. Stand.* **2014**, *20*, 448–451.
41. *ISO 21434*; Road Vehicles—Cybersecurity Engineering. ISO: Geneva, Switzerland, 2021.
42. *ISO 26262*; Road Vehicles—Functional Safety. ISO: Geneva, Switzerland, 2018.
43. *SAE J3061*; Cybersecurity Guidebook for Cyber-Physical Automotive Systems. SAE-Society of Automotive Engineers: Warrendale, PA, USA, 2016.
44. Cadzow, S.; Eichbrecht, P.; Evensen, K.; Fischer, H.J.; Davila-Gonzalez, E.; Hoefs, W.; Kargl, F.; Koenders, E.; Lykkja, O.M.; Moring, J.; et al. *EU-US Standards Harmonization Task Group Report: Summary of Lessons Learned*; No. FHWA-JPO-13-076; United States Joint Program Office for Intelligent Transportation Systems: Washington, DC, USA, 2012.
45. ETSI. *Intelligent Transport Systems (ITS); Communication Architecture for Multi-Channel Operation (MCO)*; Release 2; European Telecommunications Standards Institute: Paris, France, 2021.
46. Hubaux, J.P.; Capkun, S.; Jun, L. The security and privacy of smart vehicles. *IEEE Secur. Priv.* **2004**, *2*, 49–55. [CrossRef]
47. McKerral, A.; Pammer, K.; Gauld, C. Supervising the self-driving car: Situation awareness and fatigue during highly automated driving. *Accid. Anal. Prev.* **2023**, *187*, 107068. [CrossRef]
48. Coppola, R.; Morisio, M. Connected car: Technologies, issues, future trends. *ACM Comput. Surv. (CSUR)* **2016**, *49*, 1–36. [CrossRef]
49. Bae, J.K.; Park, M.C.; Yang, E.J.; Seo, D.W. Implementation and performance evaluation for DSRC-based vehicular communication system. *IEEE Access* **2020**, *9*, 6878–6887. [CrossRef]
50. Sheik, A.T.; Maple, C. Edge Computing to Support Message Prioritisation in Connected Vehicular Systems. In Proceedings of the 2019 IEEE Global Conference on Internet of Things (GCIoT), Dubai, United Arab Emirates, 4–7 December 2019; pp. 1–7. [CrossRef]
51. McEnroe, P.; Wang, S.; Liyanage, M. A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges. *IEEE Internet Things J.* **2022**, *9*, 15435–15459. [CrossRef]
52. Montanaro, U.; Fallah, S.; Dianati, M.; Oxtoby, D.; Mizutani, T.; Mouzakitis, A. On a fully self-organizing vehicle platooning supported by cloud computing. In Proceedings of the 2018 Fifth International Conference on Internet of Things: Systems, Management and Security, Valencia, Spain, 15–18 October 2018; pp. 295–302.
53. Stevens, A.; Dianati, M.; Katsaros, K.; Han, C.; Fallah, S.; Maple, C.; McCullough, F.; Mouzakitis, A. Cooperative automation through the cloud: The CARMA project. In Proceedings of the 12th ITS European Congress, Strasbourg, France, 19–22 June 2017; pp. 1–6.
54. Arthurs, P.; Gillam, L.; Krause, P.; Wang, N.; Halder, K.; Mouzakitis, A. A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6206–6221. [CrossRef]
55. Gillam, L.; Katsaros, K.; Dianati, M.; Mouzakitis, A. Exploring edges for connected and autonomous driving. In Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; pp. 148–153.
56. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
57. Javed, A.M.; Zeadally, S.; Hamid, Z. Trust-based security adaptation mechanism for Vehicular Sensor Networks. *Comput. Netw.* **2018**, *137*, 27–36. [CrossRef]

58. Al-Sultan, S.; Al-Doori, M.M.; Al-Bayatti, A.H.; Zedan, H. A comprehensive survey on vehicular ad hoc network. *J. Netw. Comput. Appl.* **2014**, *37*, 380–392. [CrossRef]
59. Raw, R.S.; Kumar, M.; Singh, N. Security challenges, issues and their solutions for VANET. *Int. J. Netw. Secur. Its Appl.* **2013**, *5*, 5.
60. Arena, F.; Pau, G.; Severino, A. A review on IEEE 802.11 p for intelligent transportation systems. *J. Sens. Actuator Netw.* **2020**, *9*, 22. [CrossRef]
61. Wahlström, J.; Skog, I.; Händel, P. Smartphone-based vehicle telematics: A ten-year anniversary. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2802–2825. [CrossRef]
62. Siegel, J.E. *CloudThink and the Avacar: Embedded Design to Create Virtual Vehicles for Cloud-Based Informatics, Telematics, and Infotainment*; Massachusetts Institute of Technology: Cambridge, MA, USA, 2013.
63. Cho, K.Y.; Bae, C.H.; Chu, Y.; Suh, M.W. Overview of telematics: A system architecture approach. *Int. J. Automot. Technol.* **2006**, *7*, 509–517.
64. Hou, J.; Chen, G.; Huang, J.; Qiao, Y.; Xiong, L.; Wen, F.; Knoll, A.; Jiang, C. Large-Scale Vehicle Platooning: Advances and Challenges in Scheduling and Planning Techniques. *Engineering* 2023, *in press*. [CrossRef]
65. Taylor, S.J.; Ahmad, F.; Nguyen, H.N.; Shaikh, S.A. Vehicular platoon communication: Architecture, security threats and open challenges. *Sensors* **2023**, *23*, 134. [CrossRef] [PubMed]
66. Brooks, D.J. What is security: Definition through knowledge categorization. *Secur. J.* **2010**, *23*, 225–239. [CrossRef]
67. Fischer, R.; Edward Halibozek, M.; Halibozek, E.P.; Walters, D. *Introduction to Security*; Butterworth-Heinemann: Oxford, UK, 2012.
68. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* **2017**, *2*, 155–184. [CrossRef]
69. Roman, R.; Lopez, J.; Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Gener. Comput. Syst.* **2018**, *78*, 680–698. [CrossRef]
70. *ISO 27000*; Information Technology, Security Techniques, Information Security Management Systems. ISO: Geneva, Switzerland, 2020.
71. Hamida, E.B.; Javed, M.A. Channel-Aware ECDSA Signature Verification of Basic Safety Messages with K-Means Clustering in VANETs. In Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Crans-Montana, Switzerland, 23–25 March 2016.
72. Guzman, Z. Hackers Remotely Kill Jeep's Engine on Highway. Available online: https://www.cnbc.com/2015/07/21/hackers-remotely-kill-jeep-engine-on-highway.html (accessed on 20 August 2023).
73. Liu, N.; Nikitas, A.; Parkinson, S. Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. *Transp. Res. Part F Traffic Psychol. Behav.* **2020**, *75*, 66–86. [CrossRef]
74. Hariharan, J.; Sheik, A.; Maple, C.; Beech, N.; Atmaca, U. Customers' perception of cybersecurity risks in E-commerce websites. In Proceedings of the International Conference on AI and the Digital Economy (CADE 2023), Venice, Italy, 26–28 June 2023.
75. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX Security Symposium (USENIX Security 11), San Francisco, CA, USA, 10–12 August 2011.
76. Bendiab, G.; Hameurlaine, A.; Germanos, G.; Kolokotronis, N.; Shiaeles, S. Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 3614–3637. [CrossRef]
77. Nie, S.; Liu, L.; Du, Y. Free-fall: Hacking tesla from wireless to can bus. *Briefing Black Hat USA* **2017**, *25*, 1–16.
78. Tencent Security Keen Lab. Experimental Security Assessment of BMW Cars by KeenLab. Available online: https://bit.ly/34ICOBC (accessed on 20 August 2023).
79. Tencent Security Keen Lab. Tencent Security Keen Lab: Experimental Security Assessment of Mercedes-Benz Cars. Available online: https://bit.ly/34Gpqhj (accessed on 20 August 2023).
80. Ghosal, A.; Sagong, S.U.; Halder, S.; Sahabandu, K.; Conti, M.; Poovendran, R.; Bushnell, L. Truck platoon security: State-of-the-art and road ahead. *Comput. Netw.* **2021**, *185*, 107658. [CrossRef]
81. Pekaric, I.; Sauerwein, C.; Haselwanter, S.; Felderer, M. A taxonomy of attack mechanisms in the automotive domain. *Comput. Stand. Interfaces* **2021**, *78*, 103539. [CrossRef]
82. Ali, I.; Gervais, M.; Ahene, E.; Li, F. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs. *J. Syst. Archit.* **2019**, *99*, 101636. [CrossRef]
83. Zhao, M. Advanced driver assistant system, threats, requirements, security solutions. *Intel Labs* **2015**, 2–3 .
84. Radanliev, P.; De Roure, D.; Page, K.; Van Kleek, M.; Santos, O.; Maddox, L.; Burnap, P.; Anthi, E.; Maple, C. Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars. *Saf. Extrem. Environ.* **2020**, *2*, 219–230. [CrossRef]
85. Erdogan, G.; Garcia-Ceja, E.; Hugo, Å.; Nguyen, P.H.; Sen, S. A Systematic Mapping Study on Approaches for Al-Supported Security Risk Assessment. In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 12–16 July 2021; pp. 755–760.
86. Patel, A.R.; Liggesmeyer, P. Machine learning based dynamic risk assessment for autonomous vehicles. In Proceedings of the 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), Rome, Italy, 12–14 November 2021; pp. 73–77.
87. Ali, E.S.; Hasan, M.K.; Hassan, R.; Saeed, R.A.; Hassan, M.B.; Islam, S.; Nafi, N.S.; Bevinakoppa, S. Machine learning technologies for secure vehicular communication in internet of vehicles: Recent advances and applications. *Secur. Commun. Netw.* **2021**, *2021*, 8868355. [CrossRef]

88. Yuan, E.; Esfahani, N.; Malek, S. A systematic survey of self-protecting software systems. *ACM Trans. Auton. Adapt. Syst. (TAAS)* **2014**, *8*, 1–41. [CrossRef]
89. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; Technical Report; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
90. UCISA. Privacy Impact Assessment Toolkit. Available online: https://www.ucisa.ac.uk/PIAToolkit (accessed on 20 August 2023).
91. Azam, N.; Michala, L.; Ansari, S.; Truong, N.B. Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR's Perspective. *IEEE Trans. Big Data* **2022**, *9*, 388–414. [CrossRef]
92. Huang, H.; Li, H.; Shao, C.; Sun, T.; Fang, W.; Dang, S. Data redundancy mitigation in V2X based collective perceptions. *IEEE Access* **2020**, *8*, 13405–13418. [CrossRef]
93. Tremblay, J.; Prakash, A.; Acuna, D.; Brophy, M.; Jampani, V.; Anil, C.; To, T.; Cameracci, E.; Boochoon, S.; Birchfield, S. Training deep networks with synthetic data: Bridging the reality gap by domain randomization. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, Salt Lake City, UT, USA, 18–22 June 2018; pp. 969–977.
94. Skygo. Security Research Report on Mercedes Benz Cars—SkyGo Blog. Available online: https://skygo.360.net/archive/Security-Research-Report-on-Mercedes-Benz-Cars-en.pdf (accessed on 20 August 2023).
95. Thoughts, B.Y. Man Block ETC with Melon Seed Bags and Evades Fees 22 Times over 40,000 in 3 Months. Available online: https://www.youtube.com/watch?v=Bzw7pA0rHCk (accessed on 20 August 2023).
96. Curry, S. More Car Hacking! Available online: https://twitter.com/samwcyo/status/1597792097175674880 (accessed on 20 August 2023).
97. Finkle, J.; Woodall, B. Researcher Says Can Hack GM's OnStar App, Open Vehicle, Start Engine. Available online: https://www.reuters.com/article/us-gm-hacking-idUSKCN0Q42FI20150730 (accessed on 20 August 2023).
98. Lodge, D. Hacking the Mitsubishi Outlander Phev Hybrid. Available online: https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/ (accessed on 20 August 2023).
99. Computest. Car Hack Project Volkswagen/Audi. Available online: https://www.computest.nl/en/knowledge-platform/rd-projects/car-hack/ (accessed on 20 August 2023).
100. Tencent. Tesla Model S Wi-Fi Protocol Stack Vulnerability. Available online: https://v.qq.com/x/page/v304513meir.html (accessed on 20 August 2023).
101. BlackHat. Multiple Vulnerabilities Disclosed in Black Hat Europe VW ID Series. Available online: https://www.blackhat.com/eu-22/ (accessed on 20 August 2023).
102. Vakhter, V.; Soysal, B.; Schaumont, P.; Guler, U. Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet Things J.* **2022**, *9*, 13338–13352. [CrossRef]
103. Arif, M.; Wang, G.; Bhuiyan, M.Z.A.; Wang, T.; Chen, J. A survey on security attacks in VANETs: Communication, applications and challenges. *Veh. Commun.* **2019**, *19*, 100179. [CrossRef]
104. Francillon, A.; Danev, B.; Capkun, S. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 24–28 April 2011; Volume 2011.
105. Norte, J.C. Hacking Industrial Vehicles from the Internet. Available online: http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html (accessed on 20 August 2023).
106. Mazloom, S.; Rezaeirad, M.; Hunter, A.; McCoy, D. A Security Analysis of an In-Vehicle Infotainment and App Platform. In Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT 16), Austin, TX, USA, 8–9 August 2016.
107. Obzy. BMW 330I 2011 Format String DOS Vulnerability (CVE-2017-9212). Available online: https://twitter.com/__obzy__/status/864704956116254720 (accessed on 20 August 2023).
108. CISA. ICS Advisory. Available online: http://shorturl.at/fhp78 (accessed on 20 August 2023).
109. Samcurry. Cracking My Windshield and Earning $10,000 on the Tesla Bug Bounty Program. Available online: https://bit.ly/3XXgJFC (accessed on 20 August 2023).
110. Cylect. Dosla—Tesla Vulnerability—CVE-2020-10558 | Cylect.io. Available online: https://cylect.io/blog/cybr-2/dosla-tesla-vulnerability-cve-2022-10558-1 (accessed on 20 August 2023).
111. NIST. CVE-2020-28656 Detail. Available online: https://nvd.nist.gov/vuln/detail/CVE-2020-28656 (accessed on 20 August 2023).
112. GeekPwn. Find a Few Key Keys on Google, and Then Crack Your Own Car? Available online: https://mp.weixin.qq.com/s/-xlV8nPjIy5nUT4Zt4a5rg (accessed on 20 August 2023).
113. Dengdeng. Many Car Owners in Shanghai Were Reminded That "There Is a Gunfight on the Road"? Available online: https://mp.weixin.qq.com/s/Zc-_Z0PyZQ8qSvZEXU2U3Q (accessed on 20 August 2023).
114. Hoppe, T.; Kiltz, S.; Dittmann, J. Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. *Reliab. Eng. Syst. Saf.* **2011**, *96*, 11–25. [CrossRef]
115. Sgayou. Subaru Starlink Persistent Root Code Execution. Available online: https://github.com/sgayou/subaru-starlink-research (accessed on 20 August 2023).
116. Garip, M.T.; Gursoy, M.E.; Reiher, P.; Gerla, M. Congestion attacks to autonomous cars using vehicular botnets. In Proceedings of the NDSS Workshop on Security of Emerging Networking Technologies (SENT), San Diego, CA, USA, 8 February 2015.
117. Liu, J. Belgian Security Researchers from KU Leuven and IMEC Demonstrate Serious Flaws in Tesla Model X Keyless Entry System. Available online: https://bit.ly/3XJa81V (accessed on 20 August 2023).

118. Zehavi, I.; Shamir, A. Facial Misrecognition Systems: Simple Weight Manipulations Force DNNs to Err Only on Specific Persons. *arXiv* **2023**, arXiv:2301.03118.
119. Nassi, B.; Nassi, D.; Ben-Netanel, R.; Mirsky, Y.; Drokin, O.; Elovici, Y. Phantom of the Adas: Phantom Attacks on Driver-Assistance Systems. Cryptology ePrint Archive. 2020. Available online: https://eprint.iacr.org/2020/085 (accessed on 22 October 2023).
120. Petit, J.; Stottelaar, B.; Feiri, M.; Kargl, F. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Eur.* **2015**, *11*, 995.
121. Yan, C.; Xu, W.; Liu, J. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con* **2016**, *24*, 109.
122. Deng, Y.; Zhang, T.; Lou, G.; Zheng, X.; Jin, J.; Han, Q.L. Deep learning-based autonomous driving systems: A survey of attacks and defenses. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7897–7912. [CrossRef]
123. Muhammad, K.; Ullah, A.; Lloret, J.; Del Ser, J.; de Albuquerque, V.H.C. Deep learning for safe autonomous driving: Current challenges and future directions. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 4316–4336. [CrossRef]
124. Pham, M.; Xiong, K. A survey on security attacks and defense techniques for connected and autonomous vehicles. *Comput. Secur.* **2021**, *109*, 102269. [CrossRef]
125. Meng, Q.; Hsu, L.T.; Xu, B.; Luo, X.; El-Mowafy, A. A GPS spoofing generator using an open sourced vector tracking-based receiver. *Sensors* **2019**, *19*, 3993. [CrossRef]
126. Narain, S.; Ranganathan, A.; Noubir, G. Security of GPS/INS based on-road location tracking systems. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 587–601.
127. CyberRegulus. Tesla Model S and Model 3 Prove Vulnerable to GPS Spoofing Attacks as Autopilot Navigation Steers Car off Road, Research from Regulus Cyber Shows. Available online: https://bit.ly/3kNhRgM (accessed on 20 August 2023).
128. Bitsight. Bitsight Discovers Critical Vulnerabilities in Widely Used Vehicle GPS Tracker. Available online: https://bit.ly/3je70fd (accessed on 20 August 2023).
129. AnonymousTV. The Largest Taxi Service in Russia 'Yandex Taxi' Was Hacked by the #Anonymous Collective. Available online: https://twitter.com/YourAnonTV/status/1565555525378506752 (accessed on 20 August 2023).
130. Mitre. CVE-2020-15912. Available online: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15912 (accessed on 20 August 2023).
131. Foster, I.; Prudhomme, A.; Koscher, K.; Savage, S. Fast and vulnerable: A story of telematic failures. In Proceedings of the 9th USENIX Workshop on Offensive Technologies (WOOT 15), Washington, DC, USA, 10–11 August 2015.
132. Burakova, Y.; Hass, B.; Millar, L.; Weimerskirch, A. Truck Hacking: An Experimental Analysis of the SAE J1939 Standard. In Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT' 16), Austin, TX, USA, 8–9 August 2016; Volume 16, pp. 211–220.
133. Kumar, K.N.; Vishnu, C.; Mitra, R.; Mohan, C.K. Black-box adversarial attacks in autonomous vehicle technology. In Proceedings of the 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington, DC, USA, 13–15 October 2020; pp. 1–7.
134. Denis, K. Remotely Controlled EV Home Chargers—The Threats and Vulnerabilities. Available online: https://securelist.com/remotely-controlled-ev-home-chargers-the-threats-and-vulnerabilities/89251/ (accessed on 20 August 2023).
135. Tencent. Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars. Available online: https://bit.ly/3XIZhos (accessed on 20 August 2023).
136. Xie, G.; Yang, L.T.; Yang, Y.; Luo, H.; Li, R.; Alazab, M. Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 4467–4477. [CrossRef]
137. Smith, C. *2014 Car Hackers Handbook-Open Garages*. 2014 . Available online: https://www.oreilly.com/library/view/the-car-hackers/9781457198847/ (accessed on 22 August 2023).
138. Verdult, R.; Garcia, F.D.; Ege, B. Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer. In Proceedings of the USENIX Security Symposium, Washington, DC, USA, 14–16 August 2013; pp. 703–718.
139. Sina. Volvo, BYD, etc. Were Exposed to the Defect of Anti-Theft System with 1 Minute Keyless Unlocking. Available online: https://finance.sina.com.cn/consume/puguangtai/20151125/155223849739.shtml (accessed on 20 August 2023).
140. Greenberg, A. Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob. Available online: https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/ (accessed on 20 August 2023).
141. Rosenblatt, S. This Hack Could Take Control of Your Ford—The Parallax. Available online: https://www.the-parallax.com/hacker-ford-key-fob-vulnerability/ (accessed on 20 August 2023).
142. Seth, R. This App Can Track Tesla Model 3 Location. Available online: https://www.the-parallax.com/tesla-radar-model-3-phone-key-ibeacon/ (accessed on 20 August 2023).
143. Kunnamon. TBONE: A Zero-Click Exploit for Tesla MCUs. Available online: https://kunnamon.io/tbone/ (accessed on 20 August 2023).
144. John, D. Canadian Software Developer Discovers Bluetooth Key Vulnerability That Allows Anyone to Unlock a Tesla. Available online: https://bit.ly/408iH88 (accessed on 20 August 2023).
145. HackingIntoYourHeart. Unoriginal Rice Patty Is My Personal Title for the Replay-Based Attack on Honda and Acura Vehticles. Available online: https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty (accessed on 20 August 2023).

146. ReverseKevin. Honda Civic Replay Attack. Available online: https://www.youtube.com/watch?v=NjbjepeILrk (accessed on 20 August 2023).
147. Pompel123. Firmware to Open Any and All Tesla Vehicle Charging Ports in Range! Available online: https://github.com/pompel123/Tesla-Charging-Port-Opener (accessed on 20 August 2023).
148. Sharma, A. Honda Bug Lets a Hacker Unlock and Start Your Car via Replay Attack. Available online: https://www.bleepingcomputer.com/news/security/honda-bug-lets-a-hacker-unlock-and-start-your-car-via-replay-attack/ (accessed on 20 August 2023).
149. Khan, S. Technical Advisory—Tesla Ble Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks. Available online: https://bit.ly/3DiuZ3M (accessed on 20 August 2023).
150. Trifinite. Project Tempa. Available online: https://trifinite.org/stuff/project_tempa/ (accessed on 20 August 2023).
151. Rollingpwn. Rolling Pwn Attack. Available online: https://rollingpwn.github.io/rolling-pwn/ (accessed on 20 August 2023).
152. Clatworthy, B. Luxury Cars Are Gone in 90 Seconds with Thief Kit. Available online: https://www.thetimes.co.uk/article/luxury-cars-are-gone-in-90-seconds-with-thief-kit-z300g0njf (accessed on 20 August 2023).
153. Blackberry. QNX-2021-001 Vulnerability in the C Runtime Library Impacts BlackBerry QNX Software Development Platform (SDP), QNX OS for Medical, and QNX OS for Safety. Available online: https://support.blackberry.com/kb/articleDetail?articleNumber=000082334 (accessed on 20 August 2023).
154. Oka, D.K.; Furue, T.; Langenhop, L.; Nishimura, T. Survey of vehicle IoT bluetooth devices. In Proceedings of the 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 17–19 November 2014; pp. 260–264.
155. VDECert. SWARCO: Critical Vulnerability in CPU LS4000. Available online: https://cert.vde.com/de/advisories/VDE-2020-016/ (accessed on 20 August 2023).
156. Sohu. An Online Car-Hailing Driver Was Jailed for Stealing Electricity 382 Times in Half a Year Using the 'Pinch Gun Method' and 'Card Second Method'. Available online: https://www.sohu.com/a/259418261_391288 (accessed on 20 August 2023).
157. Whittaker, Z. Mercedes-Benz App Glitch Exposed Car Owners' Information to Other Users. Available online: https://bit.ly/3HdD7Uh (accessed on 20 August 2023).
158. Beardsley, T. R7-2017-02: Hyundai Blue Link Potential Info Disclosure (Fixed): Rapid7 blog. Available online: https://www.rapid7.com/blog/post/2017/04/25/r7-2017-02-hyundai-blue-link-potential-info-disclosure-fixed/ (accessed on 20 August 2023).
159. Hunt, T. Controlling Vehicle Features of Nissan Leafs across the Globe via Vulnerable Apis. Available online: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/ (accessed on 20 August 2023).
160. Schneider. Schneider Electric Security Notification. Available online: https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-194-06 (accessed on 20 August 2023).
161. XiunoBBS. Vulnerability Mining Practice of Charging Piles. Available online: https://bbs.kanxue.com/thread-272546.htm (accessed on 20 August 2023).
162. Di, W. Information on 100,000 Citroen Owners May Have Been Leaked. Available online: http://shorturl.at/beSTV (accessed on 20 August 2023).
163. Xxdesmus. Honda Motor Company Leaks Database with 134 Million Rows of Employee Computer Data. Available online: https://rainbowtabl.es/2019/07/31/honda-motor-company-leak/ (accessed on 20 August 2023).
164. ZDNET. Mercedes-Benz Onboard Logic Unit (OLU) Source Code Leaks Online. Available online: https://www.zdnet.com/article/mercedes-benz-onboard-logic-unit-olu-source-code-leaks-online/ (accessed on 20 August 2023).
165. Valdes-Dapena, P. Volkswagen Hack: 3 Million Customers Have Had Their Information Stolen | CNN Business. Available online: https://edition.cnn.com/2021/06/11/cars/vw-audi-hack-customer-information/index.html (accessed on 20 August 2023).
166. MBUSA. Mercedes-Benz USA Announces Initial Findings of Data Investigation Affecting Customers and Interested Buyers. Available online: https://bit.ly/3wS6Hu5 (accessed on 20 August 2023).
167. Volvo. Notice of Cyber Security Breach by Third Party. Available online: https://www.media.volvocars.com/global/en-gb/media/pressreleases/292817/notice-of-cyber-security-breach-by-third-party-1 (accessed on 20 August 2023).
168. Asia, N. Toyota Halts Operations at All Japan Plants due to Cyberattack. Available online: https://asia.nikkei.com/Spotlight/Supply-Chain/Toyota-halts-operations-at-all-Japan-plants-due-to-cyberattack (accessed on 20 August 2023).
169. Denso. Notice of Unauthorized Access to Group Company: Newsroom: News: Denso Global Website. Available online: https://www.denso.com/global/en/news/newsroom/2022/20220314-g01/ (accessed on 20 August 2023).
170. Redazione. La Ferrari è Stata Colpita dal Ransomware Ransomexx. 7 GB di Dati Scaricabili Online. Available online: https://www.redhotcyber.com/post/la-ferrari-e-stata-colpita-dal-ransomware-ransomexx-7gb-di (accessed on 20 August 2023).
171. Nio. Statement on Data Security Incidents. Available online: https://app.nio.com/app/web/v2/share_comment?id=2284166&type=essay (accessed on 20 August 2023).
172. Puthal, D.; Nepal, S.; Ranjan, R.; Chen, J. Threats to networking cloud and edge datacenters in the Internet of Things. *IEEE Cloud Comput.* **2016**, *3*, 64–71. [CrossRef]
173. Huiyu, W. X-in-the-Middle: Attacking Fast Charging Electric Vehicles. Available online: https://conference.hitb.org/hitbsecconf2021ams/sessions/x-in-the-middle-attacking-fast-charging-electric-vehicles/ (accessed on 20 August 2023).
174. Eckert, S. Replay Attack: Numerous Traffic Lights in Germany Are Vulnerable to Manipulation. Available online: https://twitter.com/sveckert/status/1600443031915663360 (accessed on 20 August 2023).

175. Topman, N.; Adnane, A. Mobile applications for connected cars: Security analysis and risk assessment. In Proceedings of the NOMS 2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 25–29 April 2022; pp. 1–6.
176. Santhosh, J.; Sankaran, S. Defending against sybil attacks in vehicular platoons. In Proceedings of the 2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, 16–19 December 2019; pp. 1–6.
177. Nazat, S.; Abdallah, M. Anomaly Detection Framework for Securing Next Generation Networks of Platoons of Autonomous Vehicles in a Vehicle-to-Everything System. In Proceedings of the 9th ACM Cyber-Physical System Security Workshop, Melbourne, Australia, 19 July 2023; pp. 24–35.
178. Zeng, W.; Khalid, M.A.; Chowdhury, S. In-vehicle networks outlook: Achievements and challenges. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 1552–1571. [CrossRef]
179. Wolf, M.; Willecke, A.; Müller, J.C.; Garlichs, K.; Griebel, T.; Wolf, L.; Buchholz, M.; Dietmayer, K.; van der Heijden, R.W.; Kargl, F. Securing CACC: Strategies for mitigating data injection attacks. In Proceedings of the 2020 IEEE Vehicular Networking Conference (VNC), New York, NY, USA, 16–18 December 2020; pp. 1–7.
180. Li, K.; Lu, L.; Ni, W.; Tovar, E.; Guizani, M. Cooperative secret key generation for platoon-based vehicular communications. In Proceedings of the ICC 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019; pp. 1–6.
181. Wang, Z.; Wei, H.; Wang, J.; Zeng, X.; Chang, Y. Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey. *Sustainability* **2022**, *14*, 12409. [CrossRef]
182. Bianchin, G.; Pasqualetti, F. Time-delay attacks in network systems. *Cyber-Phys. Syst. Secur.* **2018**, 157–174.