sensors

MDPI

Article

Securing Cloud-Assisted Connected and Autonomous Vehicles: An In-Depth Threat Analysis and Risk Assessment

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: As threat vectors and adversarial capabilities evolve, Cloud-Assisted Connected and Autonomous Vehicles (CCAVs) are becoming more vulnerable to cyberattacks. Several established threat analysis and risk assessment (TARA) methodologies are publicly available to address the evolving threat landscape. However, these methodologies inadequately capture the threat data of CCAVs, resulting in poorly defined threat boundaries or the reduced efficacy of the TARA. This is due to multiple factors, including complex hardware–software interactions, rapid technological advancements, outdated security frameworks, heterogeneous standards and protocols, and human errors in CCAV systems. To address these factors, this study begins by systematically evaluating TARA methods and applying the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privileges (STRIDE) threat model and Damage, Reproducibility, Exploitability, Affected Users, and Discoverability (DREAD) risk assessment to target system architectures. This study identifies vulnerabilities, quantifies risks, and methodically examines defined data processing components. In addition, this study offers an attack tree to delineate attack vectors and provides a novel defense taxonomy against identified risks. This article demonstrates the efficacy of the TARA in systematically capturing compromised security requirements, threats, limits, and associated risks with greater precision. By doing so, we further discuss the challenges in protecting hardware–software assets against multi-staged attacks due to emerging vulnerabilities. As a result, this research informs advanced threat analyses and risk management strategies for enhanced security engineering of cyberphysical CCAV systems.

Keywords: threat analysis; threat modeling; risk assessment; cyber security; connected vehicles; autonomous vehicles; edge computing; cloud; taxonomy; attack tree; countermeasures

Citation: Sheik, A.T.; Maple, C.; Epiphaniou, G.; Dianati, M. Securing Cloud-Assisted Connected and Autonomous Vehicles: An In-Depth Threat Analysis and Risk Assessment. *Sensors* **2024**, *24*, 241. https://doi.org/10.3390/s24010241

Academic Editors: Kien Nguyen and Xiaoyan Wang

Received: 23 October 2023
Revised: 4 December 2023
Accepted: 14 December 2023
Published: 31 December 2023

1. Introduction

Cloud-Assisted Connected and Autonomous Vehicles (CCAVs) are at the forefront of vehicular technology, integrating cloud services, edge computing, Roadside Units (RSU), and various Connected and Autonomous Vehicle (CAV) models [1–3]. Operating on complex hardware and software platforms, these systems are the subject of ongoing research aimed at bolstering security and safety. With rapid technological evolution, CCAVs face heightened security risks, particularly from threats that can compromise security requirements like confidentiality, integrity, availability, authenticity, authorization, and accountability [4–6]. This paper focuses on delineating these security threats, encompassing both targeted and multistaged attacks on the hardware and software systems of CCAVs. This study systematically identifies and analyses complex threats, conducts an in-depth risk assessment, and formulates comprehensive countermeasures [7]. The aim is to enhance understanding of these emerging threats and contribute to the development of robust security strategies for CCAV systems.

A prior system-centric survey of the CCAV threat landscape using a platooning use case has led to formulating and mapping an attack taxonomy [8]. The survey identified

132 threats from the literature, 64 real-life security breaches, and 22 threats specific to platooning microservices. The results highlight limitations, open challenges, and the need for future work that implements threat analysis and risk assessment (TARA) methods in the broader CCAV ecosystem. TARA methods provide a systematic approach to modeling CCAVs [9], which aid the identification of strengths and weaknesses in their systems by assessing their impact.

Research on reference architectures for CCAVs, particularly regarding their implementation and operation with edge/cloud and cloud environments, is in the early stages [4,5]. Although an increasing number of theoretical, lab-based, and real-world attacks are known, these have not been considered or analyzed in the CCAV context but have been surveyed in [8]. As a result, it is important to contribute to this field by formulating a research-based reference architecture for CCAVs to systematically perform TARA in order to capture the threats exposed to the assets in the system.

This study aims to systematically examine and quantify risks to CCAV systems and explore the issues associated with securing CCAVs effectively. This was achieved through completing the following objectives: (1) analyze architectures for CCAVs; (2) perform a systematic threat analysis and risk assessment to evaluate the impact on trust domains and security requirements; and (3) suggest countermeasures on trust domains using a defense taxonomy by mapping hardware and software components of CCAV systems.

The remainder of this paper is organized in the following manner: Section 2 presents an overview of the three-tier architecture system, offering contextual information. In Section 3, an examination of the TARA methods is conducted to facilitate the comparison and analysis of different approaches. In Section 4, an adversarial model is presented, which examines the motivations, capabilities, and opportunities of various threat actors in the context of developing threats and evaluating their associated risks. In this study, Section 5 provides an in-depth description of the research methodology used. Section 6 of the document focuses on the examination of the TARA. This section provides a comprehensive overview of the system architecture, the outcomes of the STRIDE/DREAD analysis, the trust domains that are affected, and the security requirements that arise from these findings. Section 7 covers an examination and discourse on the identified threats, vulnerabilities, and implications on security requirements, accompanied by a discussion of the constraints inherent in the methodology, resulting in the formulation of an attack tree. Section 8 of the document places emphasis on countermeasures, organizing them into distinct categories using a defense taxonomy and subsequently offering a comprehensive analysis. In conclusion, Section 9 serves as the concluding section of this research paper.

2. Background

CAVs require real-time data exchange and processing, and delays incurred by limited onboard computing hardware capabilities are potentially dangerous. A notable advancement in this area has been Cloud-Assisted Real-Time Methods for Autonomy (CARMA), a project financed by the EPSRC and Jaguar Land Rover. CARMA uses an Internet-of-Things (IoT)-inspired three-tier architecture (see Figure 1), suitable for mission-critical and time-sensitive applications. Each tier has different functions: (i) Tier 1—CCAVs: These vehicles are designed to process data locally while maintaining communication with edge clouds or RSUs through Cooperative Awareness Messages (CAMs); (ii) Tier 2—Core Cloud; The core cloud handles the computing for mission planning, mobile infrastructure management, security and database management, map management, and third-party applications, while also offering services to the edge cloud; and (iii) Tier 3—Edge Cloud: The edge cloud performs off-board vehicular computation, regional map analysis, and security algorithms such as authentication. By leveraging powerful infrastructures like the core cloud and third-party services, the edge cloud can execute latency-free localized computations for CCAVs; however, this increases the attack surface.

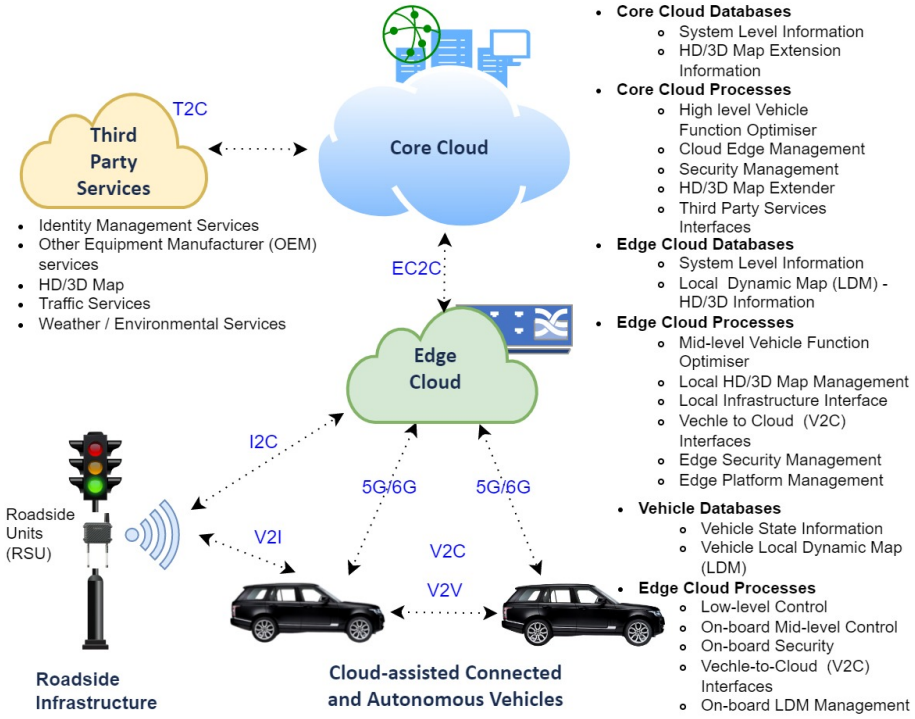

Figure 1. High-level view of Cloud-Assisted Connected and Autonomous Vehicles, adapted from [5,10,11].

3. Threat Analysis and Risk Assessment Methods

TARA is a systematic technique used to model CCAV applications and trust domains and mitigate risks in these systems through a thorough and valid evaluation of the current state of the system [12]. The complexity of CCAV ecosystems makes them vulnerable to targeted multistage cyberattacks, which can have a significant impact on both hardware and software components. The TARA considers this challenge of identifying and understanding attack paths to effectively deploy appropriate safeguards. The TARA may employ formal techniques such as data flow diagrams (DFDs), attack trees, MITRE ATT&CK, tactics, techniques, and procedures to analyze threats. Alternatively, they may adopt methods explored in literature, including advanced techniques such as discrete-time Markov chains, state-space models, and Bayesian networks; however, the latter is not adopted in this research due to the evolving nature of the landscape. As such, this research used the data collected from literature and real-life incidents from previous research available in [8]. On the basis of these data, this research considered the following approaches to perform the TARA.

3.1. Microsoft's STRIDE/DREAD

The widely adopted STRIDE technique, developed by Microsoft as part of the Security Development Lifecycle, serves to identify, describe, and analyze threats, their impacts, as well as entry points and vectors on the trust domains of the system [9]. It benefits organizations by allowing them to respond to changes throughout the lifespan of the system. The term STRIDE corresponds to (1) Spoofing (S)—the process of forging the identity of a person or a system. It may be directed towards a configuration, a file, a machine, sensory data or system, or a person's specific function. Spoofing compromises authenticity. (2) Tampering (T)—the process of modifying data to induce an error in the system's functioning. It may be directed at individual files, sensory data, or whole networks and compromises integrity. (3) Repudiation (R)—a method of eradicating traces of system activity related to log files. Repudiation compromises non-repudiation. (4) Information Disclosure (I)—the process of gaining unauthorized access to the data storage or data flow. This compromises

confidentiality. (5) Denial of Service (D)—the process of interfering with or disturbing normal functioning. Denial of Service compromises availability. (6) Elevation of Privilege (E)—the process of performing an unauthorized action in the system, compromising access and authorization.

STRIDE can be adapted to CyberPhysical Systems (CPSs) by deconstructing them into logical and physical components, considering the interplay of internal and external units. This helps to develop DFDs for each of these components. It adds authenticity, nonrepudiation, safety, and authorization to the standard CIA (Confidentiality, Integrity, and Availability) [13].

DREAD was created to assist STRIDE in risk assessment [6]. It presents a categorisation-based technique for assessing risks using Equation (1) and the adversarial model discussed in Section 4, which is based on (1) Damage Potential (D)—the assessment of the damage inflicted on a system by a cyberattack. (2) Reproducibility (R)—the assessment of the means through which a cyberattack may be replicated. For example, if an assault can be repeated, it poses a serious danger to the system. (3) Exploitability (E)—the assessment of the feasibility of conducting a cyberattack in comparison to the requirements for successful execution. (4) Affected Users (A)—the evaluation that takes into account the potential effect of the attack on the number of users. (5) Discoverability (D)—the examination that takes into account the attack's discoverability inside the system.

$$Risk = (D + R + E + A + D)/5 \quad (1)$$

3.2. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

OCTAVE is a risk-based technique developed by the Software Engineering Institute, the CERT Division [14,15]. OCTAVE has two broad methods. These are OCTAVE-S and OCTAVE Allegro. OCTAVE focuses on mitigating organizational risks with interdisciplinary approaches, including senior executives, operational managers, and security professionals. The process is divided into three stages: (i) establishing asset-based threat profiles for organizational security assessment; (ii) identification of infrastructure vulnerabilities; and (iii) designing a cybersecurity plan based on the identified threats to important assets.

3.3. Process for Attack Simulation and Threat Analysis (PASTA)

The PASTA considers security requirements to identify the most credible threats to a system while balancing and adhering to business goals. It provides a systematic framework that includes creating detailed documentation of the considered system. This can be labor-intensive compared with other threat modeling methods and may be challenging for developers to understand. The process involves (i) defining business and security goals and the impact of security measures on the organization, (ii) defining the technological scope, (iii) decomposition of system security, (iv) creating DFDs, (v) evaluating threats based on the security decomposition and diagrams, (vi) assessing system vulnerabilities and weaknesses, (vii) modeling potential cyberattacks, and (viii) evaluating the resulting risks and their impact on business [16].

3.4. Composite Threat Modeling

The US Department of Transportation and National Highway Traffic Safety Administration created the Composite Threat Modeling approach exclusively for vehicles that are connected and/or autonomous [17]. This methodology is divided into two stages: (i) identifying important components and (ii) analyzing the respective threats to those components. This enables security measures to be tailored based on the criticality of the threat. The technique demands that DFDs be represented with all physical or networked components, entry/exit points, and data formats. Following this, threats may be recognized by analyzing the DFDs with the purpose of identifying (i) critical data flows needed for the mission; (ii) direct/indirect data flow that may affect a critical component; (iii) the

components changing the data in the network; (iv) the physical/wireless threat entry points; and (v) the security properties of the system.

3.5. Attack Tree

The ability to detect, assess, and visualize threats is crucial for CCAVs. In terms of complexity, it can be difficult to fully understand the intricacies involved in an attack pathway. To tackle this issue, researchers have suggested using attack trees to visually represent cyber attacks. These representations offer a comprehensive view of the steps and components involved in a cyber attack. Despite their benefits, there is currently a lack of consistency in how attack trees are depicted. To enhance their effectiveness, it is essential to establish a unified representation. Therefore, while attack trees can be very useful in visualizing threats in CCAVs, they must be standardized for the improved perception, understanding, and representation of detected threats from CCAVs [18].

3.6. Analysis of TARA Techniques

We considered five potentially relevant threat modeling methods for a CCAV ecosystem [19]. It is difficult to address all the challenges of such a use case with a single solution [20]. Therefore, a selection of metrics developed from the work in [21] were used to assess the methods in this research: (i) Maturity: Is the technique well-defined and has it been employed in earlier research? (ii) Adaptability: Is the technique adaptable to the unique needs of the use case? (iii) Safety and Security Dependency Coverage: Is the technique inclusive of the implications of safety and security? (iv) Hardware and Software Threats: Does the analysis include both hardware and software threats? (v) Documentation: Does the technique have an extensive documentation?

Evaluating various methodologies for cyber threat detection enables objective analysis, highlighting their respective strengths and weaknesses. Table 1 summarizes the considerations based on the defined metrics. Comparisons are drawn between Attack Tree, Composite Threat Modeling, PASTA, OCTAVE, and STRIDE/DREAD. Composite Threat Modeling, PASTA, and STRIDE/DREAD utilize DFDs in their frameworks, which is helpful in analyzing attack paths and affected components in CCAVs. STRIDE/DREAD, PASTA, and Attack Trees demonstrate higher adaptability for new use cases and both are capable of capturing threats from reference architecture. However, PASTA requires extensive organizational consultation. Thus, STRIDE/DREAD and Attack Tree are followed for the rest of this study. The following section discusses the considered adversarial model, research methodology, results, and analysis.

Table 1. Evaluation of the threat modeling methods (M: Maturity, A: Adaptability, SS: Safety and Security Dependency, H/S: Hardware and Software Threats, D: Documentation).

Method	M	A	SS	H/S	D
Attack Trees [22]	✓	✓		✓	✓
Composite Threat Modeling [17]	✓		✓	✓	✓
OCTAVE [15]	✓				✓
PASTA [16]	✓	✓		✓	✓
STRIDE DREAD [9]	✓	✓	✓	✓	✓

4. Adversarial Model

Adversaries exploit vulnerabilities for a variety of reasons and incentives; see Table 2. An attacker may be aggressive or passive, external or internal, and may have malicious or subjective motives. Individuals may be members of loosely coordinated groups, organizations, and foreign or domestic government agencies. They may be motivated by

financial gain, vengeance, ideological views, cyberwarfare, or they may be an intellectual challenge [23]. There are two basic scenarios that an attacker might exploit: operational and technological. Operational scenarios are described as attacks (multistaged or targeted) that occur over a given timeframe and include both technical and operational components throughout the detect–mitigate–respond stages of an attack scenario. These are often more complex and follow a low-and-slow attack technique that relies heavily on human input and intuition in the strategy. Technical (proactive) scenarios are mostly concerned with network anomalies and disruption.

Table 2. Adversarial model.

Expertise	Threat Actor	Motivation	Capability	Opportunity	Threat	DREAD
Layman	Solo—Outsider	Personal satisfaction; Passion; Ideology.	Limited	Minimal	S	Damage Potential —If a threat exploit occurs, evaluate the damage caused 0 = Nothing 2.5 = Individual user data compromised 5=Complete system or data destruction
Proficient	Solo—Insider	Financial gain; Discontent	Moderate to High	Internal knowledge	T	*Reproducibility*—How easy is it to reproduce the threat exploit? 0 = Very hard or impossible even for administrators/DBAs 2.5 = One or two steps required, may need an authorized user 5 = Just a web browser is enough
	Group—Ad hoc	Dependant on group purpose: Ideological,financial, political	Limited to Moderate	Limited knowledge and financial	R	
Expert	Group—Established	Dependant on group purpose: Ideological, financial, political	Limited and Moderate knowledge	Moderate to High	I	*Exploitability*—What is needed to exploit this threat? 0 = Advanced programming networking knowledge 2.5 = Malware exists on the Net, or any tolls available 5 = Just a web browser is enough
Multiple experts	Organization—Competitor	Corporate espionage; Financial gain; Reputation damage	Moderate to High	Limited and moderate knowledge and financial and contextual	D	*Affected Users*—How many users are affected? 0 = None 2.5 = Some users, but not all 5 = All users
	Organization—Partner	Information gain; Financial gain			E	*Discoverability*—How easy is it to discover the threat. 0 = Very hard or impossible; needs source code or admin access 2.5 = Can figure it out by guessing or monitoring network traces 5 = Information is visible in the web browser or address bar or in the form or as a hidden variable
Intelligence RD	Nation-State	State rivalry; Geopolitics	High	High knowledge, finance and advance skills and resources		

In summary, an adversary targeting the CCAV and its ecosystem should have the capability to study, practice, and instrument an attack by reverse engineering, modifying, replacing, and remotely injecting malicious codes that alter firmware and software pertaining to respective hardware in the cloud-assisted architecture for CAVs [24,25]. The following are the attributes of an adversary that have been considered for this research:

- *Threat Agent:* The adversarial entity that has set its aims on a particular victim.
- *Motivation:* The attacker's motivations in terms of the benefit he seeks by carrying out the attack.
- *Adversary Capability:* Distinct capability and skills of the adversary.
- *Opportunity:* Indicates the resources and opportunities that are required for the group of threat agents to identify and exploit the vulnerability.
- *Threat:* A cyberattack is a hostile act intended to harm, steal, or disrupt digital assets. A cyber threat is an attempt to obtain unauthorized access to, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or other sensitive data.
- *Tactic:* Tactics are the most abstract level of the MITRE ATT&CK technique. They are the tactical objectives pursued by an adversary during an attack.
- *Technique:* The ATT&CK model's tactics outline an adversary's goal. Each tactic category has an endless variety of techniques and subtechniques.

5. Research Methodology

Our research methodology uses STRIDE-DREAD to analyze impacted trust domains. We first establish the DFDs for CCAVs, cloud, and edge cloud to enable a more in-depth analysis of threats. The DFDs are described in Tables A1, A3 and A5, which detail each

trust domain process, threat entries, and its impact. Our data came from research into real-life incidents (R) and threats detailed in the literature (L), as discussed in [8].

With this knowledge of trust domains and threats, we performed the STRIDE-DREAD analysis on each trust domain. We determined the potential impact of threats found through R and L and classified them as high, medium, and low risks. To understand the risk distribution of threats on trust domains, we demonstrated our results using pie charts. Then, we demonstrated compromised security requirements and assessed the risks by creating Sankey charts.

The outcome of our STRIDE/DREAD analysis for *L* and *R* was mapped. This mapping facilitated the development of an attack tree, which indicates the attack pathways to compromise a CCAV system. After systematically assessing the threats to CCAV security, we created a defense taxonomy that summarizes the countermeasures against attack mechanisms, which were identified in [8]. This helped us in better understanding the validity of overlaps between *L* and *R*, while mapping with the hardware and software measures. Finally, we suggested immediate countermeasures.

Recognizing the importance of comprehensive methods in ensuring the validity and reliability of our findings, certain improvements can be made in our methodology. Firstly, our data collection procedures will be iteratively reassessed and updated to further improve the representativeness of our sample. In the interest of minimizing bias further, we examine and control for potential confounding variables and refine our experimental design to further reduce errors and increase accuracy. Furthermore, our methodology will benefit from integrating Advanced Persistent Threats (APT) and the use of Machine Learning (ML) and Deep Learning (DL) to perform threat ranking to increase its capability to assess qualitative and quantitative threat-related information in a single set of processes. These improvements are aimed at significantly strengthening the longevity and credibility of our study as part of future work.

6. Results

This section presents the findings derived from the CCAV model in detail. The respective findings are detailed in (a) System Architecture, (b) STRIDE/DREAD, (c) Impacts on Trust Domains, (d) Impacts on Security Requirements, (e) Risk-Based Classification of Trust Domains with Attack Mechanisms.

6.1. System Architecture

Figure 2 illustrates the operational aspects of CCAVs with trust domains, which were identified in [8]. It broadly comprises Devices and Peripherals, CAV systems, Cloud and Edge Cloud, Radio FM/AM/DAB, and Drivers and Passengers. The system comprises subcomponents that interact among themselves. It captures both the internal and external connections of components of CCAVs, with a focus on the key assets utilized in conjunction with infrastructure-enhanced cooperative cruise control application [11]. To achieve this, the study adapts reference architecture originally proposed by [5], customizing it for a three-tier architecture that suits the specific requirements of CCAVs. This is performed to simplify the complex network, identify trust domains, and analyze potential threats.

The DFD shows how CCAVs operate by communicating internally with Electronic Control Units (ECUs) to actuate brakes, steering, and the infotainment system. Controller Area Network (CAN), FlexRay, Media Oriented System Transport (MOST), and Local Interconnect Network (LIN) communication protocols link different ECUs to endpoints such as Tyre Pressure Monitoring Systems (TPMS), infotainment systems, cameras, LIDAR, RADAR, brakes, and actuators [26]. Details of the data flow and the 11 trust domains are described in Table A1.

Similarly, Figures 3 and 4 demonstrate the functions of edge cloud and cloud for CCAVs, which aids threat examination [26]. The systems comprise 12 trust domains for edge cloud and 8 trust domains for cloud. These include Devices and Peripherals, as well as Roadside Infrastructures for Edge Cloud and Cloud. Tables A2 and A3 present a detailed overview

of the data flow paths and processes within trust domains, including descriptions of these domains and the potential threat entry/exit points for both the cloud and edge cloud.

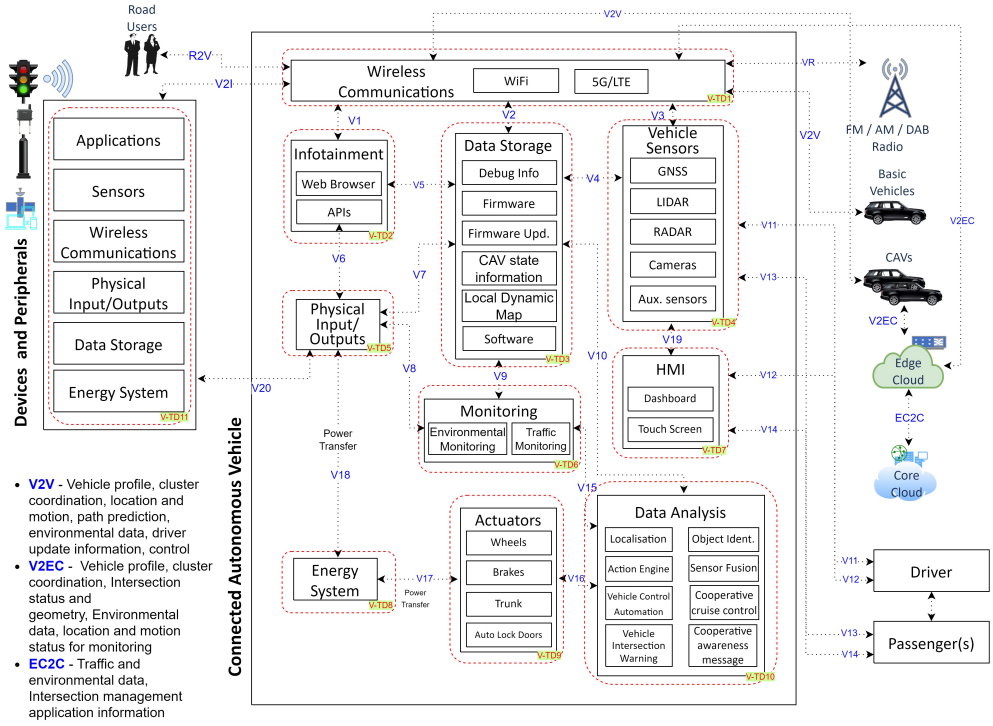

Figure 2. Cloud-Assisted Connected and Autonomous Vehicles Architecture.

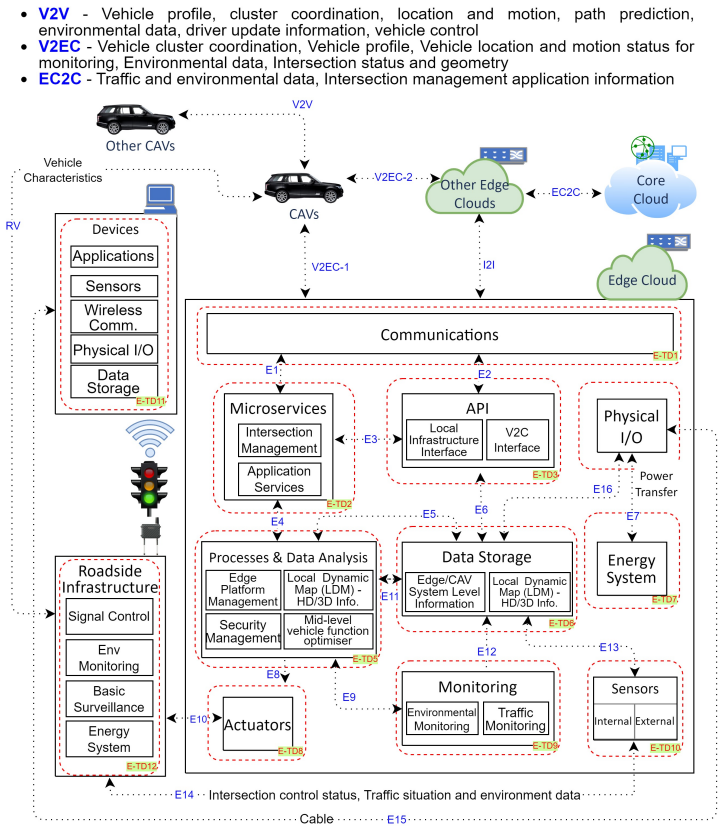

Figure 3. Cloud-Assisted Connected and Autonomous Vehicles—Edge cloud architecture.

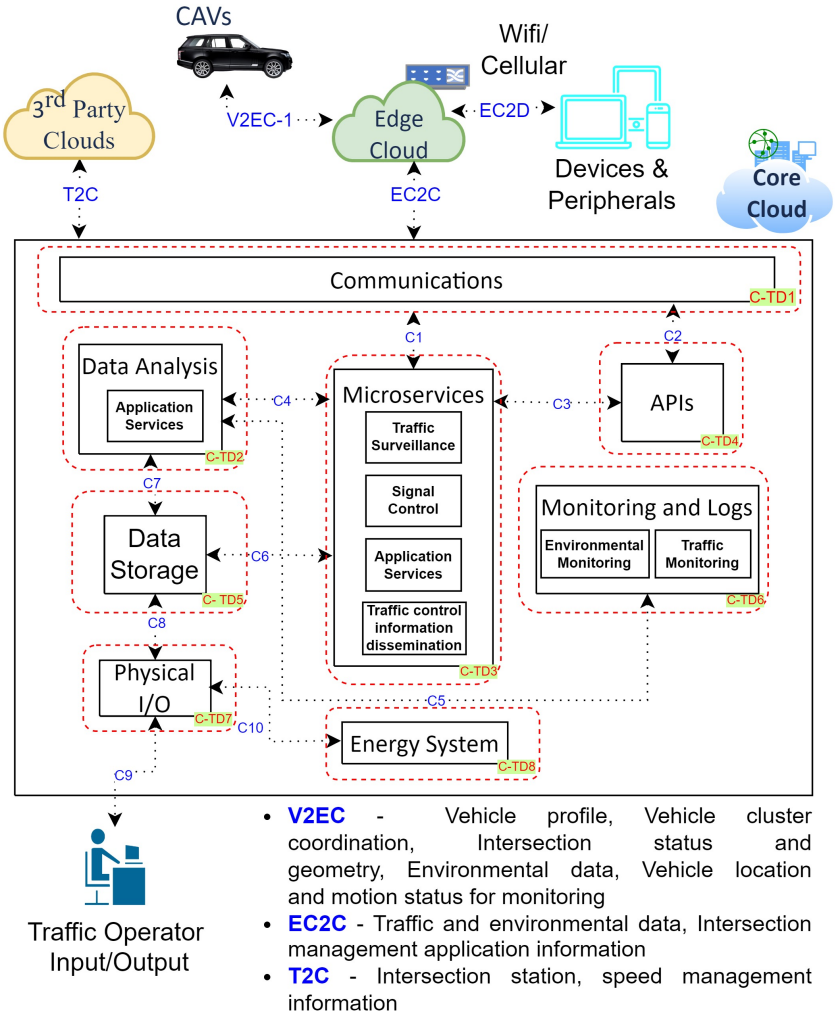

Figure 4. Cloud-Assisted Connected and Autonomous Vehicles—Cloud architecture.

6.2. STRIDE-DREAD

Our evaluation has measured the severity of risks linked to the detected threats using the DREAD methodology on a 5-point scale, as shown in Equation (1). Threats with an average DREAD value of 3.8 or more are classified as High-risk, those between 2.8 and 3.8 are considered Medium-risk, and those scoring less than 2.8 are deemed Low-risk threats. After identifying the threats from the literature review and applying STRIDE methodology, a further investigation of 63 real-life attacks between the year 2015 and the end of 2022 on CAVs was carried out and detailed in [8]. These threats assist in validating the literature review threats. Tables A4 and A5 summarize and list the types of CCAV attacks that have been studied, predicted, and conducted on systems that compromise confidentiality, integrity, and availability [25,27–34]. The following observations, shown in Table 3, were collected throughout the TARA phases from the threats initially exposed to the CCAV system. Further details on the threats and their classification based on identified attack vectors can be referred to in Figure A1.

Table 3. The number of threats categorised as Low (Caution-Blue), Medium (Warning-Yellow), or High (Critical-Red).

	Low	Medium	High
Literature Review Threats			
CAVs	2	40	34
Edge/Cloud and Cloud	7	37	12
Real-Life Threats			
CAVs	3	47	36
Edge/Cloud and Cloud	1	14	17

6.3. Impact on Trust Domains

This study concentrates solely on the threats sourced from the Literature and Real Life. Upon analysis, we found that a single identified threat could have the potential to compromise multiple trust domains. The averaged values of risk levels on the impacted trust domains due to the identified threats from both the Literature review and Real Life are represented in the pie chart shown in Figure 5.

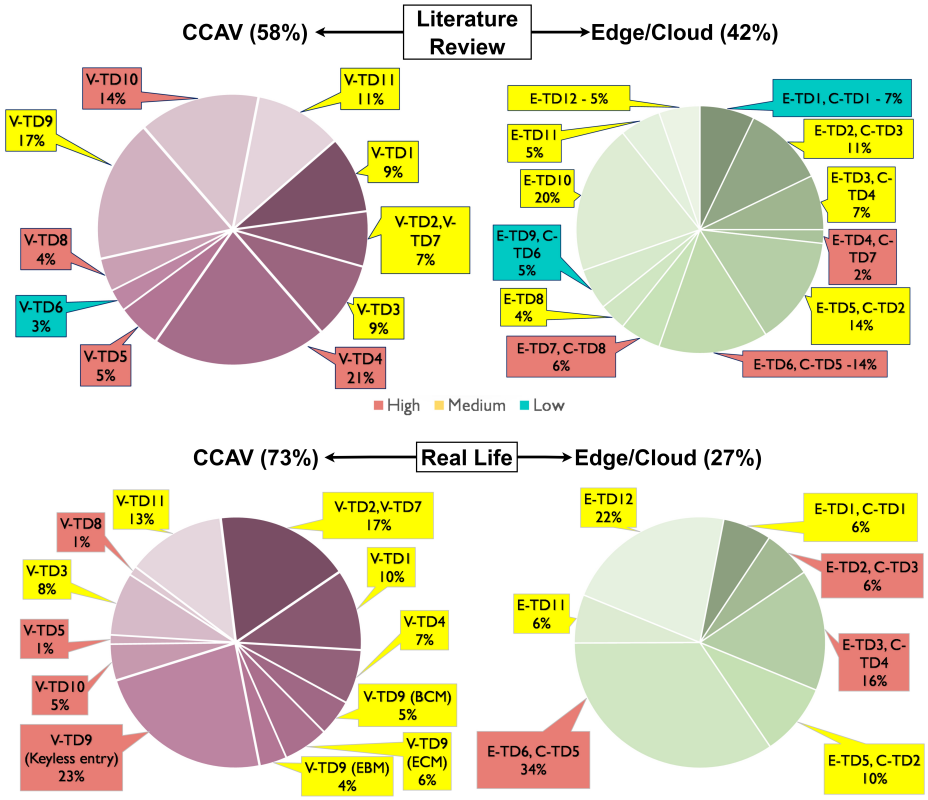

Figure 5. Literature review and Real-Life threat—analysis.

Within the CCAV system, 44% of detected Literature threats are classified as high risk, primarily affecting the V-TD4 Vehicle's Sensors, V-TD5 Physical Input/Output, V-TD8 Energy System, and V-TD10 Data Analysis. Similarly, 30% of the identified Real-Life threats are considered high-risk and have significant implications on V-TD5 Physical Input/Output, V-TD8 Energy System, V-TD9 Keyless Entry System, and V-TD10 Data Analysis trust domains. This study underscores the reality that, despite their identification through research, these high-risk vulnerabilities continue to be exploited in real-world scenarios, presenting a pressing problem that requires immediate attention.

In the context of edge/cloud systems, 22% of the Literature threats are identified as high-risk, predominantly affecting E-TD4, C-TD7 Physical Input/Output, E-TD6, C-

TD5 Data Storage, and the E-TD7, C-TD8 Energy System. On the contrary, Real-Life threats suggest that 56% of attacks significantly impact E-TD2, C-TD3 Microservices, E-TD3, C-TD4 APIs, and E-TD6, C-TD5 Data Storage, with Data Storage alone accounting for 34%. These findings illustrate the discrepancies in the affected trust domains, with Data Storage emerging as the most frequently targeted. This vulnerability could stem from the escalating competition for data and antagonistic interests targeting stored data. Another contributing factor might be the relatively slow commercial adoption of Edge/Cloud technologies for CCAV applications, hinting at the possibility of future threats that could lead to operational failures in the system.

When it comes to Literature threats in CCAVs, a small percentage of 3% carries a low risk to the V-TD6 Monitoring module, whereas 12% displays low risks for the E-TD1, C-TD1 Wireless Communication Modules, as well as the E-TD9, C-TD6 Actuator modules. However, no low-risk Real-Life threats have been identified within the CCAV systems. One potential explanation for these observations is that these types of attacks might not be widely reported in mainstream media due to strategic decisions made by organizations to mitigate potential harm to their reputation.

The residual 53% of the Literature threats on CCAVs and 66% on Edge/Cloud collectively constitute the medium-risk category. Intriguingly, our analysis did not find any Real-Life threat reports related to V-TD8 Energy Systems for CCAV or E-TD4, C-TD7 Physical Input/Output, E-TD7, C-TD8 Energy Systems, E-TD8 Actuators, E-TD9, C-TD6 Monitoring, and E-TD10 Sensors for Edge/Cloud trust domains. The remaining Real-Life threats across other trust domains exhibit medium risks, accounting for 70% for CCAVs and 44% for Edge/Cloud systems.

The results highlight that a substantial portion of both the Literature and Real-Life threats on CCAVs and Edge/Cloud systems fall within the medium risk category. Furthermore, the results suggest that while theoretical models predict vulnerabilities in these areas, they may not yet have been exploited or reported in real-life scenarios. Overall, these insights emphasize the need for ongoing research and proactive threat management strategies, particularly in high-risk areas and emerging technologies. They also highlight the value of comprehensive threat reporting, without which our understanding of vulnerabilities in CCAV systems would remain nonexistent.

6.4. Impact on Security Requirements

Figures 6 and 7 present an examination of trust domains, STRIDE threats, security requirements, and risk severity related to CCAVs and Edge/Cloud systems. This study also recognizes privacy as a key requirement, as represented in the Sankey diagrams. This is an evolving area of research. Historically, privacy and security were perceived as mutually exclusive. These distinctions were drawn during the design and operation of systems that aimed to provide lawful data access and modifications. Decisions regarding information access and alterations in a challenging and intricate environment like CCAVs have always been distinct from considerations of security, legal compliance, and regulations. Consequently, the idea that privacy and security are not mutually exclusive has gained acceptance.

A common contention made against data privacy is that it cannot be achieved without ensuring security. However, the reverse—that security implies privacy—may not always hold true. Many people tend to equate a technology's effectiveness with its ability to provide privacy and security. Nevertheless, to develop new privacy and security solutions, further research is required to understand the discrepancies and synergies between these two disciplines. Consequently, this could assist in identifying elements that ensure privacy principles compatible with comprehensive CCAV security [35].

The data derived from Figure 6 indicate that CCAVs are subject to medium risks (54%), high risks (37%), and low risks (9%). It is noteworthy that there are no low-risk instances for availability and nonrepudiation. In relation to security requirements, this study reveals that breaches of confidentiality account for 10.5% of compromises, integrity breaches for 20.9%, and availability breaches for 14.9%. Additionally, breaches of authenticity and authorization

each make up 19.4% of compromises. Overall, privacy breaches represent 10.4% of the total security compromise. When it comes to the classification of threats, 26 are deemed high risk, with three of them (sensor spoofing, key/certificate replication, and Bus-off) presenting exclusively high risks. The other 23 threats also contribute to medium risks, and an additional 22 threats pose only medium-level risks. Interestingly, five of the threats classified as low risk also pose both high and medium risks to the CCAV system.

The data derived from Figure 7 for Edge/Cloud systems reveal risk patterns akin to those observed in CCAVs. Medium-level risks are the most prevalent at 53%, trailed by high-level risks at 28% and low-level risks at 19%. In terms of security requirements, the study finds that breaches of confidentiality, integrity, and availability account for 53.2% of the total compromises in Edge/Cloud systems, compared with 46.3% in CCAVs. Breaches of authenticity and authorization together contribute to 21.2% of security compromises in Edge/Cloud systems, as opposed to 38.8% in CCAVs. Notably, privacy breaches occur approximately 9% more frequently in Edge/Cloud systems compared with CCAV systems. When evaluating threats, 14 are identified as high risks in Edge/Cloud systems. Two of these threats, specifically Byzantine attack and Map database poisoning, present only high-level risks. Six threats span both medium and high-risk categories, while the remaining six impact all three risk levels. Moreover, 12 out of the remaining low-level risk threats also carry medium-level risks, and an additional 15 threats pose only medium-level risks.

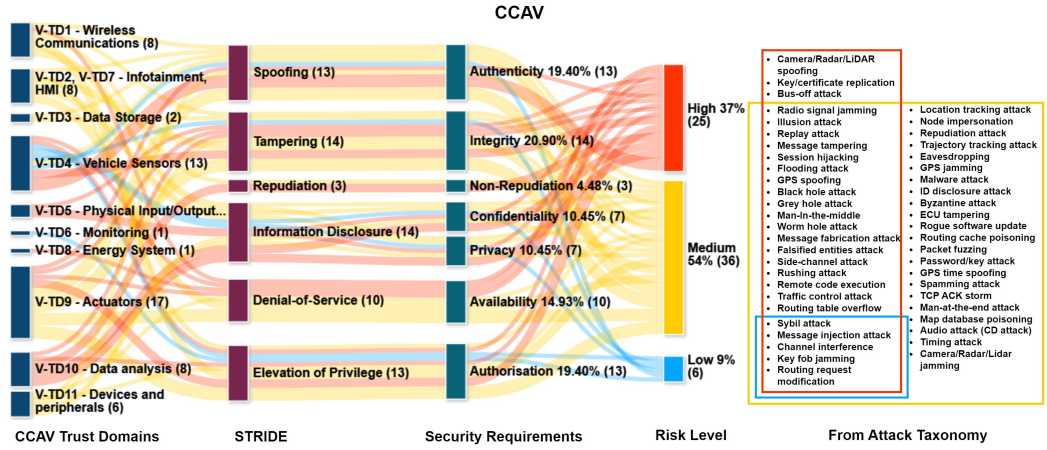

Figure 6. CCAV Sankey diagram describing respective trust domains, STRIDE, compromised security requirements, and criticality of the risk.

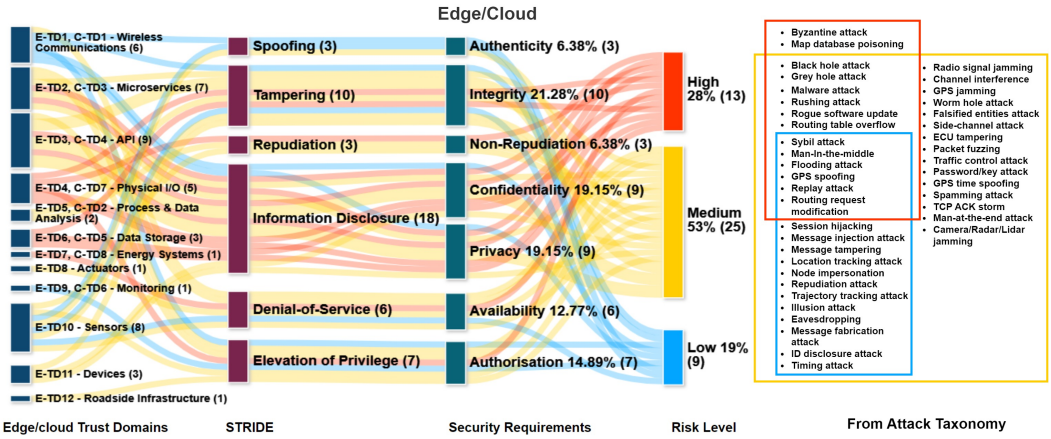

Figure 7. Edge and core cloud Sankey diagram describing respective trust domains, STRIDE, compromised security requirements, and criticality of the risk.

In summary, the findings unveil a complex and dynamic security landscape, marked by a variety of emerging threats and risks. Addressing these challenges will necessitate

comprehensive, agile, and multidimensional security strategies and frameworks that are not only capable of responding to the current threat environment but also equipped to anticipate and prepare for future developments. This implies that there is a need for continuous monitoring mechanisms with advanced predictive analytics to counteract emerging threats, which may involve machine learning and artificial intelligence. Additionally, the study highlights an imperative need for a paradigm shift in understanding and ensuring data privacy, which is often overlooked. Effective strategies would recognize the intricate relationship between security and privacy.

7. Analysis and Discussion

In this study, we executed a TARA methodology utilizing the STRIDE model to systematically capture threats and quantify risks. In addition, this research has quantified risks with the DREAD model. Limitations inherent to this approach for identifying threats in hardware and software components are discussed in this section. This technique assists in distinguishing the impact of current controls, thus enabling the identification of both strengths and weaknesses within the CCAV system. This paper also used mature CCAV reference architectures with assets identified systematically in [8]. This further enables us to learn attack pathways by constructing detailed attack trees. From this discussion, key countermeasures are developed in alignment with existing standards. This progression is crucial in guiding further research in this domain.

7.1. Threats and Risks

Threat Identification, Threat Distribution, and Refinement of Threat Understanding require further analysis to gain insight into the complex landscape of risks.

- *Threat Identification and Distribution*: This study identifies a variety of threats with some, such as Byzantine attacks and Map database poisoning, exclusively posing 'Critical'-level risks, while others affect multiple risk levels. This complexity and diversity of threats necessitate ongoing threat intelligence and assessment.
- *Risk Identification and Distribution*: This research infers high-level risks as 'Critical', medium-level risks as 'Warning', and low-level risks as 'Caution'. The findings reveal a significant proportion of 'Warning'-level risks in both CCAVs and Edge/Cloud systems, constituting 54% and 53%, respectively. While the presence of 'Critical'-level risks is indeed concerning, the dominance of 'Warning'-level risks highlights the ongoing security challenge that needs to be managed with a multilayered security strategy. The overlapping impact of threats across all risk categories ('Critical', 'Warning', and 'Caution') adds a layer of complexity to the system's security, emphasizing the need to strategise proactive measures. A threat that is considered 'Caution' or low-risk in one scenario might contribute to a 'Warning' or 'Critical'-risk situation in another, depending on the overall security context.
- *Refinement of Threat Understanding*: Through the use of attack trees, mapping potential attack routes from data flow diagrams, and referencing architecture, our comprehension of potential threats and their vectors would be improved. However, there seems to be an obscurity in the methodology to create security solutions for both hardware and software components, indicating a need for further research and development in this area.

7.2. Security Requirements

This subsection delves into the analysis concerning the potential breaches of Confidentiality, Integrity, Availability, Authenticity, Authorization, and Privacy highlighted in the Sankey diagram.

- *Confidentiality, Integrity, and Availability*: Often referred to as the CIA triad, they are revealed as the most frequently compromised security requirements, accounting for a large portion of the total security compromises in Edge/Cloud systems (53.2%) and CCAVs (46.3%). This underscores a fundamental vulnerability in the core security

architecture of these systems and the importance of strategic measures to protect the CIA triad.

- *Authenticity and Authorization*: Authenticity and authorization compromises form a smaller but significant proportion of security compromises. There is a stark difference between Edge/Cloud systems (21.2%) and CCAVs (38.8%), highlighting the unique security challenges of each system. This difference could be indicative of more complex user interaction models or greater reliance on trusted access controls in CCAVs.
- *Privacy*: Interestingly, privacy compromises occur 9% more frequently in Edge/Cloud systems compared with CCAVs, likely reflecting the shifting threat landscape driven by the value and volume of data processed by these systems. This also emphasizes the growing challenges posed by stringent data privacy regulations and the need for proactive privacy-by-design approaches.

7.3. TARA Limitations

There are several limitations of TARA when applied to CCAVs. Firstly, these methods cannot precisely represent adversarial behavior, especially in targeted or multistage attacks that exploit physical components as attack agents. The existing TARA methodologies struggle to capture the complexity of such attacks, which impairs their effectiveness in safeguarding CCAVs.

It is understandable that traditional approaches like STRIDE and DREAD would face scrutiny for their efficacy. These methods may not fully accommodate the unique security challenges presented by CCAV technology, which is rapidly evolving. Consequently, the need for more robust and comprehensive analysis techniques is necessary to ensure the security of CCAVs against emerging security threats.

A significant gap exists in the systematic security analysis of CCAVs. The focus in the field is primarily on analyzing isolated systems, disregarding the intricate interplay between hardware and software components. This approach fails to capture the vulnerabilities and potential effects that may arise from the complex interactions within a dynamic CCAV ecosystem.

Accurately characterizing the degree to which a CCAV system conforms to security requirements presents a challenge for researchers because it is difficult to define, verify, and validate conformance. In addition to this, there is a need to account for various assumptions about system performance. As a result, security requirements that are poorly defined can lead to insufficient protection against potential threats.

Despite these limitations, protecting CCAVs from identified threats is imperative. To address these challenges, it is essential to develop advanced countermeasures and analysis techniques that protect against the exploitation of CCAV vulnerabilities. The TARA methodology has been instrumental in understanding the necessity for the development and application of countermeasures on both hardware and software components of the systems. To improve our ability to recommend countermeasures, we map attack pathways and construct an attack tree in this section to learn how a CCAV could systematically be compromised. Following this, we develop a defense taxonomy that provides a step toward achieving this objective for subsequent research in the next section.

7.4. Attack Tree

The attack tree, illustrated in Figure 8, is a graphical representation of the potential security threats in a generalized CCAV scenario, with the primary source of these vulnerabilities arising from external communications within the Vehicle-to-Everything (V2X) systems. It is crucial to note that the attack tree highlights the adverse consequences of a compromised CCAV system, including the potential for collisions, thereby emphasizing the importance of ensuring the security of these systems. The attack tree validates that there are several attack vectors that show a vehicle is vulnerable through wireless channels or via the onboard system [36,37].

In summary, the findings, taxonomy, and attack tree show that CCAVs are vulnerable. To exploit a CCAV, an adversary may employ a series of attack techniques and varied tactics. The intricacies of these attack mechanisms, which range from external to internal communications, are visually represented in the attack tree shown in Figure 8. This diagram captures potential attacks that could be initiated from vehicle-to-vehicle (V2V) interfaces or from the edge cloud towards CCAVs. Such a visual representation aids in comprehending the multifaceted nature and complexity of potential attacks that could compromise the security requirements of safety-critical CCAVs by impacting specific trust domains.

As seen in Table A5, it is critical to address these issues through strong and efficient security mechanisms such as anomaly detection, tamper-resistant hardware systems, secure software development practices, and the secure segmentation of onboard vehicular networks, which is explored in the following section.

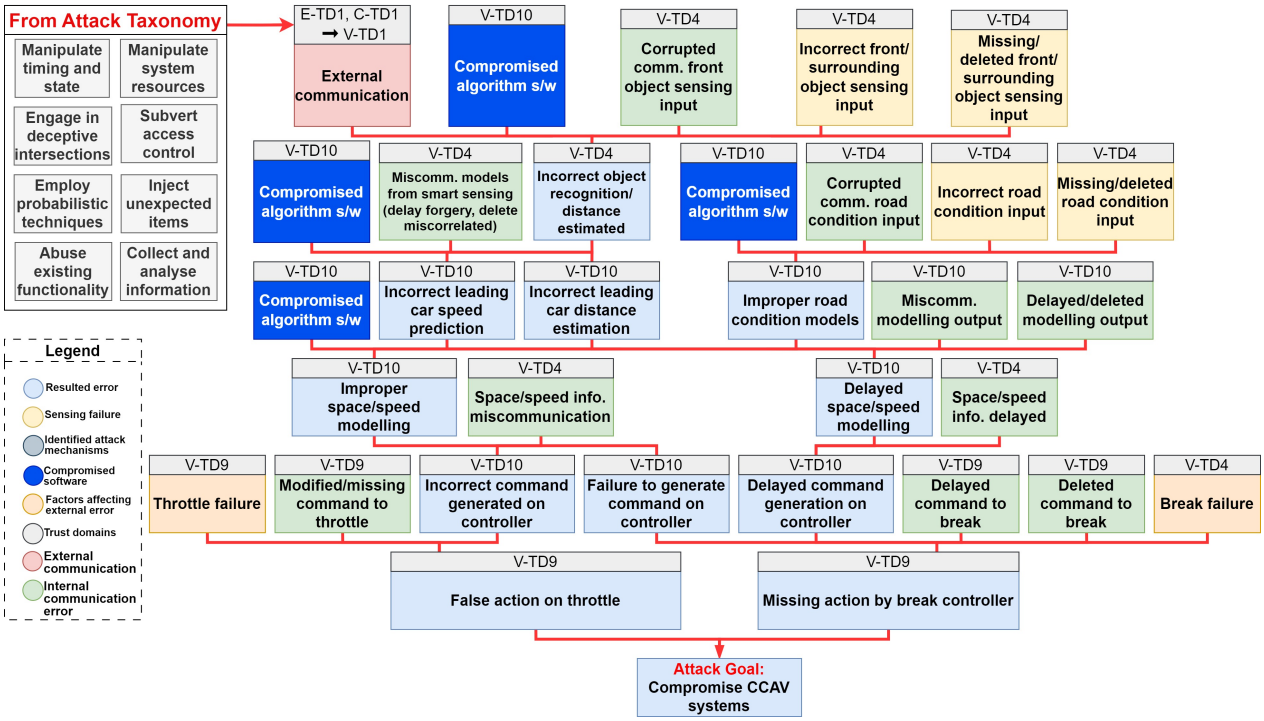

Figure 8. Attack tree capturing attacks from attack taxonomy that illustrates impacts on the generalised CCAV scenario. Further information on Attack taxonomy can be obtained from [8].

8. Countermeasures

Stringent measures can be employed to protect CCAV systems and mitigate potential risks, even in the face of unpredictable and complex threats. Our methodology identified numerous threats to both the hardware and software components of CCAV systems. While providing a high-level understanding of threats, our study focused on analyzing threats at the component level and acknowledged the challenges associated with this approach. To achieve this goal, we mapped attack mechanisms to the hardware and software components of each trust domain within a CCAV system using an Attack Tree (see Section 7). In this section, we propose a classification of hardware and software components to identify attack mechanisms and impacted trust domains. Based on these mechanisms, a defense taxonomy was developed. Drawing insights from the literature, ongoing research, and real-world implementations, we proposed key countermeasures by identifying the impacted trust domains and analyzed them.

8.1. Classification of Trust Domains with Attack Mechanisms

The TARA has enhanced our understanding of the need for tailored countermeasures for each hardware and software component. However, there is a notable obscurity in

the approach to devising security solutions for both hardware and software. To pinpoint solutions, we categorized various attacks and grouped them according to their attack mechanisms, which were clustered from the attack taxonomy illustrated in [8]. These were then correlated with the affected trust domains, granting us the insight that countermeasures can potentially be suggested based on the classification of attack mechanisms.

From Figure 9, we can derive that every identified trust domain is encompassed within the security of hardware and software components. Regarding hardware attacks, a total of 28 trust domains are affected: all 11 trust domains under the CCAV are impacted, alongside 17 of the edge and cloud trust domains, excluding the monitoring systems. Of these, 11 trust domains are identified as high risk, 14 are considered medium risk, and 3 are considered low risk based on our previous evaluations. In terms of software security, 18 trust domains are impacted: 7 are related to CCAV and the remaining 11 pertain to edge and cloud systems. Among these, six trust domains are classified as high-risk, seven as medium-risk, and four as low-risk, again, following our preceding analysis

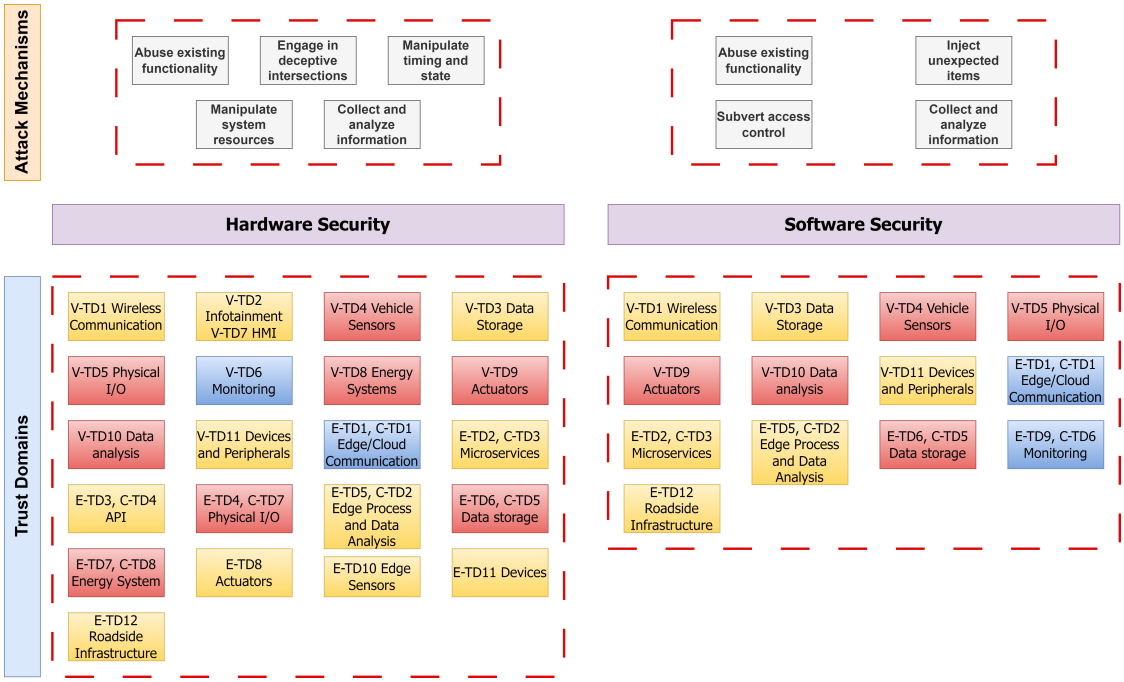

Figure 9. Mapping trust domains to attack mechanism (vectors).

8.2. Defense Taxonomy Based on Attack Mechanisms

Figure 9 underscores the need for a multifaceted strategy to safeguard trust domains in CCAV systems, entailing a blend of diverse yet interrelated countermeasures tailored to specific attack vectors. Building a defense taxonomy is a two-step process: first, mapping trust domains and then curating the taxonomy using identified attack mechanisms. An extensive list of countermeasures from Tables A4 and A5, labeled as Hardware Security *(H)* and Software Software *(S)*, is aligned to these attack mechanisms, as depicted in Figure 10. While this figure depicts a comprehensive list, the subsequent section discusses key immediate countermeasures. Further details on countermeasures for each trust domain can be referred to in Figure A2.

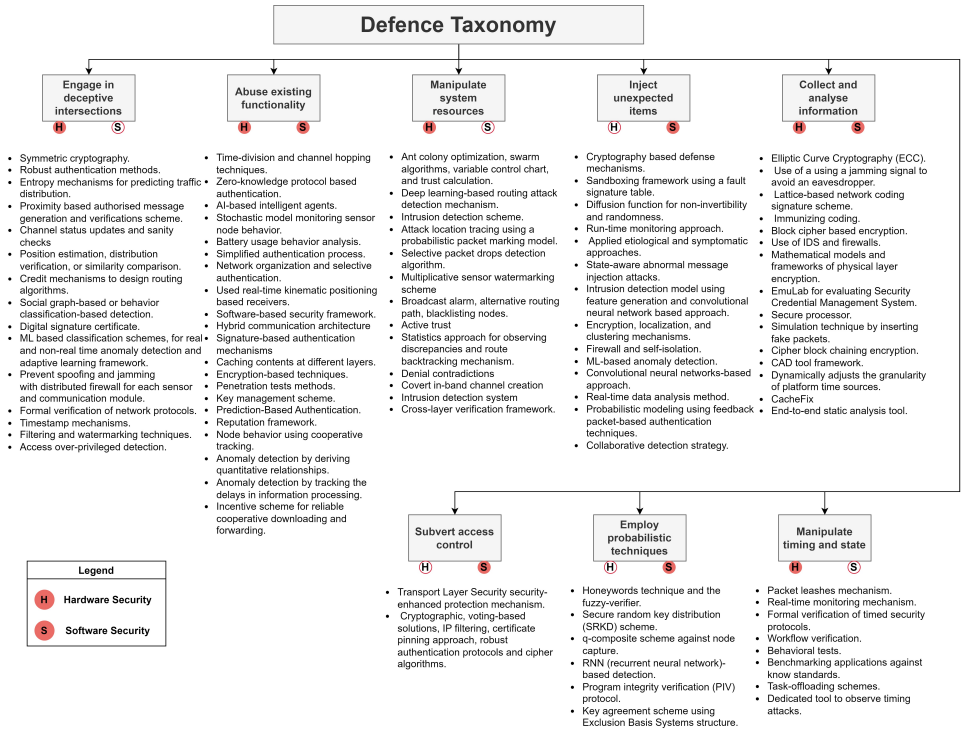

Figure 10. Defence taxonomy for CCAV attack mechanisms.

8.3. Key CCAV Countermeasures

It is important to consider key security practices when adopting new countermeasures for the secure development lifecycle of a vehicle. Miller and Valasek [26] assert that vehicles should be designed with safety prioritized and recommend defensive technologies, such as an Intrusion Detection System (IDS), to prevent attacks on the CAN bus. To detect an attack, histogram analysis of diagnostic packets during the CAN bus operation could study the repetitive nature of system messages and detect anomalies that indicate a deviation from normal operation. Moreover, the National Highway Traffic Safety Administration [38] has proposed a layered approach to harden vehicle electronics. The approach employs preventive measures by isolating safety-critical and identification systems, utilizing intrusion detection and real-time threat response, and regularly assessing comprehensive system solutions. These solutions are shared collaboratively, incorporating data from past security threats between partners and organizations.

Bariah et al. [30] discussed security mechanisms including PKI, ID-based cryptosystem, and situation-based mechanisms. PKI ensures data authentication and nonrepudiation but lacks consistent location privacy. ID-based mechanisms use user/vehicle information for verification and offer pseudonym generation for privacy but incur additional overhead. The authors found that ID-based mechanisms outperform PKI in terms of time, bandwidth, and storage. Situation-based modeling helps monitor, analyze, and ensure security but requires high computational resources for spontaneous sensing and model extraction.

Amoozadeh et al. [33] proposed countermeasures such as local plausibility checks and infusing information from external devices. However, this approach introduces additional risks and attack vectors through smartphones and wearables, which could be used to inject malicious packets into a vehicle. Limitations include unreliable smartphone processing power, trustworthiness of third-party device applications, and confidence in verifying data with onboard systems. The authors also suggested using voting as a countermeasure, where vehicles track each other's behavior to identify anomalies. However, further research is needed to improve computational and communication overheads for voting mechanisms [33].

8.3.1. Hardware Security Module

To ensure the security and trustworthiness, of CCAVs, robust hardware-based security measures are crucial. Hardware Security Modules (HSMs), or Trusted Platform Modules (TPMs), are effective in authenticating and protecting onboard systems. These specialized devices securely store and process sensitive data, preventing tampering, unauthorized access, and malware attacks. They safeguard the integrity and confidentiality of vehicle location data, sensor data, and communication keys. However, research and development have progressed privately and as such, public knowledge and understanding are limited. Proprietary solutions in the automotive industry may suppress innovation and result in legal challenges. Collaboration and liability policies among technology companies, automotive OEMs, and governments are essential for secure data logging and forensic analysis during cyber incidents [24,27,39,40].

8.3.2. Cryptographic Solutions—Encryption and Authentication

To enhance security in CCAVs and associated infrastructure systems, various encryption and authentication mechanisms have been recommended. However, implementing these techniques poses challenges due to resource constraints and limited computational power in vehicles. The complexity is exacerbated when vehicles are built containing varying hardware and software from different manufacturers. Therefore, relying on a single static security mechanism is insufficient, and multiple security mechanisms are needed for onboard and remote systems. Recent research focuses on short-term certificates, pseudonyms, and efficient revocation lists using Trusted Authorities (TA) and PKI with support from RSUs [41,42].

8.3.3. Software Updates

To address security vulnerabilities in manufactured vehicles, Over-the-Air (OTA) software updates from edge or cloud have been proposed as a solution for upgrading and fixing software vulnerabilities. While OTA updates can address onboard vulnerabilities, there is a risk of executing remote codes through malicious OTA updates. If not implemented securely, this can enable adversaries to inject malware and execute remote code [43]. Research on the probability and impact of various vulnerabilities on compromised software, hardware, and sensors in vehicles has been limited [44]. Resilience is crucial for safety-critical CCAV systems, and implementing redundant systems can enhance resilience. However, the characteristics of redundant system technologies, such as communication and perception sensors, are still unclear. Research on reliable and resilient software systems is significant but currently limited.

8.3.4. Anomaly Detection Mechanisms

Attention to cloud-based security solutions for securing CCAVs has been growing over time. Companies like HERE, Ericsson, IBM, CloudCar, GM On-Star, and Amazon AWS have previously discussed centralized cloud architectures [45]. Amazon AWS and Ericsson have proposed connected vehicle cloud systems that give anomaly detection in the cloud infrastructure greater weight in detecting malicious data packets using machine learning algorithms. Detected anomalies are stored in a local database and shared with other vehicles for notification [43,46]. Academic research suggests using vehicle trajectory, data clustering, and entropy-based attack detection to enable the systematic surveillance of anomalies among vehicles in a CCAV's three-tier architecture [47–49].

8.4. Analysis of Countermeasures

As seen in Figure 9, it is apparent that the identified trust domains encompass both hardware and software security elements. The risk levels within this cluster are diverse for both hardware and software security. This reveals the specific vulnerabilities of each element and emphasizes the necessity of specialized countermeasures for respective com-

ponent security. This suggests that a 'one-size-fits-all' approach may not be sufficient in developing robust and effective security measures.

The above points indicate the importance of a holistic, component-level security approach. Both hardware and software elements need to be shielded against potential attacks. The defensive measures should be developed based on a comprehensive understanding of the system, its components, and their vulnerabilities. This understanding, coupled with threat and risk assessments, should enable organizations to establish robust countermeasures capable of safeguarding their systems against High—'Critical', Medium—'Warning', and Low—'Caution'-level risks.

Countermeasures have been grouped based on their similarities among trust domains in CCAVs, edge cloud, and cloud, such as V-TD1, E-TD1 and C-TD1 (Wireless Communication Modules). Upon analysis, this research found various countermeasures that can protect multiple trust domains in CCAV systems against threats ranked between *low-* and *medium*-level risks and those with *medium-* to *high*-level risks:

- *Low- to Medium-Level Risks*: It is found that wireless communications can be protected from jamming attacks using preventive measures such as reactive jamming detection techniques, control channel attack prevention, trigger node identification, Hermes node, checking access rights, and TLS encryption, as well as anomaly detection techniques. This research recommends intrusion detection systems with optimized machine learning algorithms to safeguard devices, peripherals, and RSUs against adversarial attacks.
- *Medium- to High-Level Risks*: It is found that various countermeasures, such as identity management and authentication, protocol and network security, network segmentation, and Zero-Trust architecture, for protecting trust domains such as Physical Input/Output, Data Analysis, Microservice, and Sensors. In addition, the correlation of messages from neighboring vehicles and cross-verification can protect data storage, analysis, and microservices.

In summary, the authors discussed various security mechanisms for monitoring onboard network traffic in CCAVs. However, solutions addressing dynamic security features are limited, especially considering the low latency requirements of safety-critical applications in vehicles. Key areas that need attention include managing communication latency due to security overhead, minimizing message routing delays, and finding solutions for vehicle dependency on the cloud when infected with malware. There is a significant research gap in utilizing machine learning and artificial intelligence methods to predict threats and develop security mechanisms based on node behaviors; however, due to the unexplainable nature of artificial intelligence in making decisions within CCAV systems, the field remains a grave concern to passenger safety. Although there is a lack of clarity in the methodology for developing comprehensive security solutions for hardware and software. An effort was made to identify effective solutions by categorizing attacks based on attack mechanisms.

9. Conclusions

In conclusion, this paper presents a detailed study through a successful examination of the efficacy of STRIDE/DREAD in capturing security requirements and threats from a system-centric perspective in CCAVs. The objectives were successfully achieved through the formulation and analysis of CCAV architectures. A systematic threat analysis and risk assessment were conducted to evaluate the impact on trust domains and security requirements. Based on the findings, countermeasures were analyzed and suggested, utilizing a defense taxonomy that mapped the hardware and software components of CCAV systems.

This research differentiates itself from other works in the field of CCAVs, as indicated in Table 4 and Figure A3. It systematically discusses a larger number of threats in greater depth while quantifying risks, contributing to the development of novel defense taxonomy. It delves into system architecture, threats, and countermeasures to understand and protect the respective hardware-software assets, which are critical for overall system safety. By

abstracting the hardware and software components, the study investigates the security requirements of the CCAV system and its components in their ecosystem. This approach addresses a significant gap in the existing literature, particularly in the understanding of hardware–software interaction in the CCAV ecosystem, which is an open area for scientific inquiry. Future research will likely provide a better understanding of this limitation.

Table 4. Comparison with surveys related to cybersecurity of CCAVs.

Surveys	Reference Architecture	CAV	Edge/ Cloud	V2V/V2I Comm.	In-vehicle Network	Threat Analysis	Risk Assessment	Defense Taxonomy	Attack Tree	Counter Measures
[39]	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓
[25]	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
[27]	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓
[29]	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓
[50]	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
[51]	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
[23,40]	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓
[52]	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓
[53]	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
[54]	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓
[34,55]	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
[56]	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
[57]	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓
[58]	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓
[59]	✗	✗	✗	✓	✓	✓	✗	✓	✗	✓
[3]	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓
[60]	✗	✗	✗	✓	✓	✗	✗	✓	✗	✗
[61]	✗	✗	✗	✗	✓	✓	✗	✓	✗	✓
[62]	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓
[63]	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓
[64]	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓
This Paper	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

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

This paper is comprehensive because of its expansive coverage of critical topics, notably including threat analysis, risk assessment, and attack tree analysis. These elements, essential for a thorough understanding of security threats in vehicular systems, are frequently either overlooked or only partially addressed in other studies. This comprehensive inclusion sets this paper apart from other works in Table 4, like those by [39,50], which primarily concentrate on V2V/V2I communications or in-vehicle networks. Additionally, this paper broadens the scope explored in studies such as [25,29], offering a more holistic perspective on the field.

Methodologically, this paper employs STRIDE-DREAD modeling and a comprehensive literature review to analyze security threats in vehicular systems, a technique not commonly employed in studies in [60,61]. This paper's rigorous evaluation of existing literature, assessing both the strengths and limitations of prior research, aligns with but extends beyond the analyses in works like [63,64]. Furthermore, the focus on defense taxonomy and countermeasures, particularly for prioritized threats based on risk, marks a significant advancement in research. This focus, coupled with discussions of the TARA applied to detailed reference architectures, highlights this paper's comprehensive approach to addressing challenges in CCAVs. Such integration of diverse elements builds upon and enhances the foundational research conducted by scholars like [3,34,53,55,58], further solidifying this paper as a pivotal contribution to the field of CCAV security.

The proposed systematic approach for analyzing threats and risks in CCAV offers valuable insights for informed decision making in risk management. It covers important considerations for security and privacy to legal compliance, providing a foundation for future research in this field. This approach benefits stakeholders, security and privacy experts with libraries of vulnerabilities and threats, and engineers for secure coding practices with protocols. By following this approach, organizations can ensure they are in line with the latest industry standards and best practices to consider security and privacy by design.

However, there are some notable limitations to the TARA when used to analyze CCAVs. These include the inability to accurately represent complex adversarial behavior, particularly in targeted or multistage attacks that exploit physical components. Furthermore, STRIDE and DREAD may not be effective in addressing the unique security challenges of CCAV technology, which is quickly advancing. The current analysis techniques often overlook the relationship between hardware and software components and therefore fail to capture vulnerabilities due to their interaction and their potential impact within the CCAV ecosystem. The authors conclude this research with a recommendation that future research may aim to develop and employ alternative modeling techniques to analyze security threats in CCAV systems, better capture intricate vulnerabilities, and inform the latest countermeasures.

Author Contributions: Conceptualization, A.T.S. and C.M.; Methodology, A.T.S.; Software, A.T.S.; Validation, C.M. and G.E.; Formal analysis, A.T.S.; Investigation, C.M. and G.E.; Resources, A.T.S.; Data curation, A.T.S.; Writing—original draft, A.T.S.; Writing—review & editing, A.T.S., C.M. and G.E.; Visualization, A.T.S.; Supervision, C.M., G.E. 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 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 Reference Architecture—Detailed description of Trust Domains, Data Flow ID, Data Processes, Data Flow Description, Threat Entry/Exit from Figure 2.

CCAV Reference Architecture				
Trust Domain	**Data Flow ID**	**Data Process**	**Description**	**Threat Entry/Exit**
V-TD1: Wireless Communication	V2V, V2I, R2V, EC2V, VR, V1, V2, V3, VR	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.	Communication Unit (Software and Hardware modules), Antenna, V-TD2, V-TD3, TD4, Radio, EC2V, V2V, V2I
V-TD2: Infotainment	V1, V5, V6	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	Database (eg. SQL), input ports, Wifi, 5G/LTE, V-TD1, V-TD3, V-TD5
V-TD3: Data Storage	V2, V4, V5, V7, V9, V10	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.	The vehicle's sensors, monitoring module, physical input/output, and infotainment system supply these data, V-TD1, V-TD2, V-TD5, V-TD4, V-TD9
V-TD4: Vehicle Sensors	V3, V4, V11, V13, V19	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 tire pressure monitoring sensors, light sensors, parking sensors, wheel and vehicle speed sensors, and others are considered in this study.	Driver, passengers, environment, V-TD1, V-TD7
		Physical Interaction	The onboard sensors may be exposed to environment-specific threats,	Environment (e.g., fire, radiation, magnetic waves, thermal elements)
V-TD5: Physical Input/ Outputs	V6, V7, V8, V18, V20	Physical Interaction	This module refers to the physical inputs and outputs on the device, such as the USB port, the onboard diagnostic port (OBD-II), and Type 1-4 battery chargers. It is difficult to exploit these ports since they need physical access.	V-TD2, V-TD3, V-TD6, V-TD11
V-TD6: Monitoring	V7, V8, V9, V15	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 example is the black box, which is available commercially.	V-TD5, V-TD3, V-TD5, V-TD10
V-TD7: HMI	V11, V12, V13, V14, V19	Phy. interaction, data processing and 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 onboard displays.	V-TD4
V-TD8: Energy System	V17, V18	Physical Interaction	The onboard energy system may be vulnerable to environmental challenges. It mainly consists of batteries and a fuel tank (petrol or diesel)	Environment (eg. Fire, Radiation, Magnetic waves, Thermal elements), V-TD8, V-TD9
V-TD9: Actuators	V17, V16	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.	V-TD8, V-TD10
		Physical Interaction	Physical components receive their energy unit to interact with the environment	Vehicular Environment
V-TD10: Data Analysis	V10, V15, V16	Data Processing	This module is in charge of conducting an analysis on the data that have been saved. This might be for data localization, object recognition, sensor fusion and analysis, action engine decision-making, vehicle control automation, warning, and basic safety message analysis, as well as vehicular applications.	V-TD8, V-TD10
		Physical Interaction	Physical components receive their energy unit to interact with the environment	Vehicular Environment
V-TD11 Devices and Peripherals	V2I, V20	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 CCAVs 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 utilized by traffic controllers, CAVs, and other edge devices to carry out ITS-based prompts.	Environment, V2I, V20

Table A2. Edge Cloud Reference Architecture—Detailed description of Trust Domains, Data Flow ID, Data Processes, Data Flow Description, Threat Entry/Exit from Figure 3.

Edge Cloud Reference Architecture				
Trust Domain	**Data Flow ID**	**Data Process**	**Description**	**Threat Entry/Exit**
E-TD1: Wireless Communication	E1, E2, V2EC-1, I2I,	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 fiber-optic cables to the Wide Area Network (WAN).	Communication Unit (Software and Hardware modules), Antenna, E-TD2, E-TD3, CAVS, and Other Edge Clouds

Table A2. *Cont.*

Edge Cloud Reference Architecture				
Trust Domain	**Data Flow ID**	**Data Process**	**Description**	**Threat Entry/Exit**
E-TD3: API	E2, E3, E6	Data transmission and interaction	Application Program Interfaces (APIs) are used by users and software modules to obtain access to a specific service.	E-TD1, E-TD2, E-TD6
E-TD2: Microservices	E1, E3, E4	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.	E-TD1, E-TD3, E-TD5
E-TD4: Physical I/O	E15, E16, E7	Phy. interaction and 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 attacks. Users connecting over these ports should be properly authenticated, and digital records of these connection attempts should be maintained.	E-TD6, E-TD7, E-TD11
E-TD5: Process and Data Analysis	E4, E5, E11, E8, E9	Data Processing	Actuators on the edge may have an effect on the surroundings. The edge may be capable of altering the behavior and security of cars.	E-TD2, E-TD6, E-TD9
E-TD6: Data Storage	E5, E6, E11, E12, E13, E16	Database access	Data storage at the edge will be centralized in a single piece of memory hardware. Due to its exposure to manipulation, it is critical to provide safeguards such as encryption, access control, and authentication to the whole disk to prevent threats.	E-TD3, E-TD4, E-TD5, E-TD9, E-TD10
E-TD7: Energy System	E7	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-TD4
E-TD8: Actuators	E8, E10	Physical Interaction	Actuators on the edge may have an effect on the surroundings. The edge may be capable of altering the behavior and security of cars.	Environment (eg. Fire, Radiation, Magnetic waves, Thermal elements), E-TD5, E-TD12
E-TD9: Monitoring	E9, E12	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-TD5
E-TD10: Sensors	E13, E14	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-TD6, E-TD12
E-TD11: Devices	E15	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-TD4
E-TD12: Roadside Infrastructures	E10, E14, RV	Physical Interaction, Data Processing, and Transmission	COHDA units are used to represent roadside infrastructure. These devices would be utilized by traffic controllers, CAVs, and other edge devices to carry out ITS activities.	E-TD10, CAVS

Table A3. CCAV Reference Architecture—Detailed description of Trust Domains, Data Flow ID, Data Processes, Data Flow Description, Threat Entry/Exit from Figure 2.

CCAV Reference Architecture				
Trust Domain	**Data Flow ID**	**Data Process**	**Description**	**Threat Entry/Exit**
C-TD1: Wireless Communication	EC2C, T2C, C1, C2	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.	Communication Unit (Software and Hardware modules), Antenna, Third-Party Cloud Services, Edge Clouds
C-TD2: Data analysis	C4, C5, C7	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, C-TD5, C-TD6

Table A3. *Cont.*

CCAV Reference Architecture				
Trust Domain	**Data Flow ID**	**Data Process**	**Description**	**Threat Entry/Exit**
C-TD3: Microservices	C1, C3, C4	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-TD3, C-TD5, C-TD6
C-TD4: APIs	C2, C3	Physical Interaction and Data Transmission	Application Program Interfaces (APIs) are used by users and software modules to obtain access to a specific service.	C-TD1, C-TD3
C-TD5: Data Storage	C6, C7, C8	Data Processing	Edge data storage will be centralized 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-TD2, C-TD3, C-TD7
C-TD6: Monitoring and Logging	C5	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-TD2
C-TD7: Physical I/O	C9	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 are to be maintained.	C-TD5, Traffic operator input/output
C-TD8: Energy Systems	C10	Physical Interaction	Cloud data storage is vulnerable to natural disasters, power outages, cyberattacks, and human errors that can cause data loss and breaches. Energy providers must implement security measures, backups, and redundancies with disaster recovery plans while being informed of current threats.	Environment(e.g., fire, radiation, magnetic waves, thermal elements) or insider threats

Table A4. CCAV Threats (Red: High-Risk, Yellow: Medium-Risk, Blue: Low-Risk).

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
V-TD1: Wireless Communication (WiFi, Cellular, 5G/LTE)	S	• Authenticity	Wireless Communication (WiFi, 5G/LTE)	Spoofing wireless communication protocol	• Changing the code and/or file system of the Wireless Communication Module (compromising integrity) • An adversary may interrupt communication, (compromising availability)	The system must be able to detect at run-time that code has been added or changed	3	3	3	4	3	3.2
	D	Availability	Wireless Communication Module (WiFi, 5G/LTE)	Jamming wireless communication channel [65–68]	An adversary may jam the specific channel or the environment may influence the signals	Jamming detection and prevention techniques such as the following: • Channel hopping; • Reactive jamming detection techniques, control channel attack prevention; • Trigger node identification; • Hermes node.	4	4	4	5	4	4.2

Table A4. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
	E	Authorization	Wireless Communication Module (WiFi, 5G/LTE)	A malicious adversary/bot may gain additional privileges [69–71]	An adversary user may gain privileges to perform network propagation	The system must check if the access rights of the system have any malicious modifications	5	3	1	5	4	3.6
	T, R, I	Confidentiality, Non-repudiation, Integrity, Privacy	Wireless Communication Module (WiFi, 5G/LTE)	MITM in wireless communication (Frame injection, Data replay, Brute force) [54,60,70–76]	Running traditional man-in-the-middle attack tools on a suspicious twin node to intercept TCP sessions (compromising confidentiality)	TLS encryption, RADIUS authentication server	5	3	3	4	2	3.4
	E	Authorization	Long-range cellular wireless access [77]	• Long-range wireless channels cellular access using voice, 3G: This can be executed by reverse engineering protocol such as AqLink of the onboard telematics system [65] • 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 [69] • Scalability is high	• Changes the voice timeout from 12 to 60 seconds, then recalls the automobile and attacks the newly discovered buffer overflow issue. • Instructing the car to play a preprogrammed tune using the phone's microphone	• Restrict access	5	2	1	5	4	3.4
V-TD2: Infotainment, **V-TD7**: HMI	S, T, I, D, E	• Authenticity • Integrity • Confidentiality and Privacy • Integrity • Authorization	• 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 the possibility for remote access • Practical attack [66,71,73,78–87] • Scalability is small	• Indirect physical channel leading to complete control of vehicle system. • Adjust the color of interior LED lights • Show photos on the infotainment system [88] • Firmware updates [89] • Access to CAN bus and other gateways to perform alter electric window lift system, warning lights, airbag control system, and gateway ECUS [31]	• Improve code robustness • Intrusion detection techniques	5	2	2	3	5	3.4
	T, D	• Integrity and Availability	• 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 [90] • Proximity—physical Access with the possibility for remote access • Practical attack • Scalability is small	• Formatted CD due to which the system can be completely flashed with any adversarial data	• Improve code robustness • Intrusion detection techniques	3	3	3	3	4	3.2

Table A4. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
V-TD3: Data Storage	S, T	• Authenticity and Integrity	• Firmware • Firmware Update • Debug info. • Local Dynamic Map • Software [73,79,91]	• Inject fabricated frames in memory, e.g., blurry frames, wrong tags • Amend firmware to produce fabricated frames leading to the 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 [37] • Simulated attack [37] • Scalability is high [37,72,79,82,84,92]	• False warnings or services • Removed warnings or services • Delayed warnings or services	• Correlation of messages from neighboring vehicles and cross-verification • Restrict access and improve code robustness	5	2	2	3	5	3.4
V-TD4: Vehicle Sensors	S, T, E	• Authenticity, Integrity, and Authorization	Camera [77]	• Bright (250 lx) and dark (0 lx) environments, with different light sources at multiple distances (50 cm, 100 cm, 150 cm, and 200cm), presentation attack [93] • Fake env. conditions [36,94] • Physical access—close proximity to the vehicular camera • Blinding attack [95] • Phantom attack • Practical attack • Scalability is high	• Environmental light considering the light wavelength and distance between the cameras leading to incorrect model recognition [95] • Not able to tune the autoexposure	• Introduction of multiple cameras for redundancy checks • A random private signal called a 'watermark' could be added to the actuators to detect tampering in sensor measurements	5	5	5	4	5	4.8
	S, T	• Authenticity and Integrity	Ultrasonic [95]	• 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 the sensor • Practical attack • Scalability is high	• Failing to detect obstacles can lead to collisions in parking or maneuvering. • Incorrect data sensed can lead to collisions [95]	• Introducing multiple sensors for redundancy check • Random probing • Probing multiple times	5	5	4	4	5	4.6
	S	• Authenticity	LIDAR [77,96,97]	• Having a working knowledge of LIDAR and a set of transceivers, the attacker receives the LIDAR signal and relays it to the next vehicle. • Two transceivers; LUX 3 uses light with a wavelength of 905nm 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	• Introducing cost-effective redundant LIDAR sensors • Random probing • Probing multiple times • Shortening pulse period	5	5	4	4	5	4.6
	D	• Availability	Global Navigation Satellite System (GNSS) [98]	• 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	• A large number of GPS receiver modules lack robust antijamming protection. Numerous companies have built equipment to identify interfering signals. However, these defense tactics may not be effective against CAVs due to their dynamic movements [98] • Adaptive array technologies [99] • Turbo coding methods for counter jamming [100]	4	3	4	4	4	3.8

Table A4. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
	S	• Authenticity and Integrity	Global Navigation Satellite System (GNSS) [98]	• An attacker transmits erroneous yet acceptable GPS signals in order to fool GPS receivers on CAVs. Attacks begin by sending signals similar to those sent by legitimate satellites. They then progressively boost the strength of their transmissions and deflect their GPS signals from the genuine position of the target [101,102]. • Practical attack [103–105] • Remote Access • Scalability is high	• GPS device processes counterfeited signal	• Monitor GPS signal strength: average or compared between time frames [106] • Monitor the signal strength of each satellite transmission received [106] • Satellite identifying codes and the quantity of received satellite signals are monitored [106] • Time interval comparison and verification [106] • Sanity check [106]	4	3	4	4	3	3.6
	S, T, I, E	• Authenticity, Integrity, Confidentiality, Privacy, and Authorization	Auxiliary Sensors: Vehicle's custom telematics features such as UConnect. This includes onboard connectivity features using wireless sensors and CAN bus vulnerabilities	• Remote access to vehicle communication systems with the ability to flash the firmware version [26] • Availability of Uconnect's DBus Port to be open for communication • Remote access • Practical attack [87,92,107] • Scalability is high	• Incorrect data sensed, which could cause trivial vehicular impacts leading to incorrect model recognition	• Code robustness • Restricted Access to OBD and patching vulnerable software	3	3	1	3	3	2.6
V-TD5: Physical Input/Outputs	T, I	• Integrity, Confidentiality, and Privacy	• Onboard Diagnostic Port [108,109] • USB	• Replay collected CAN packets, capturing each CAV response. The modified CAN packets might then control the vehicle's behavior. This is enabled with access to the OBD port and with a Windows PC operating system capable of analyzing CAN packets [110] • Direct physical access • BUS attack • Practical attack • Scalability is small • Firmware tampering [91]	• Horn: Raise the horn continuously • Vehicle brakes: Slam brakes at any speed • Gas: Change speedometer and gas gauze at will • Engine: Cause engine to accelerate • Battery: Prevent the car from powering down and/or draining the battery • Disable seat belt notification • Disable power steering or jerk wheel • Turn headlights on or off when left in automode	• Code robustness • Restricted access to OBD port	5	4	4	3	4	4
V-TD6: Monitoring	E	• Authorization	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[111] • Remote access • Practical lab-based attack • Scalability is high	• Mispredictions of signboards	• Intrusion detection system with better machine learning algorithms that could predict images based on [94]: – Size – Angle – Focus – Context – Surface – Lightning – Depth	4	3	2	2	3	2.8
V-TD8: Energy System	D	• Availability	Energy and fuel storage, power generation	• Directed energy weapons • Electronic warfare • Adjust charging current [112]	• 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 • 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 • Other systems can deliver temporary or permanent effects against the vehicles by using a radio frequency jammer, lasers, chemical sprayers, and high-power microwaves. It can cause damage to the vehicle	• It is useful to shield a CAV system with a material with reflective and thermal properties. • If the engagement can be detected, the satellite or space orbiting vehicle can use electronic systems to jam the terminal guidance of the electronic warfare weapon • Deployment of attack sensors • Development or maintenance of electronic countermeasures and electro-optical countermeasures	5	4	1	5	5	4

Table A4. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
V-TD9: Actuators	S, T, D, E	• Authenticity, Integrity, Availability, and Authorization	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 [65,70,79,113] • Scalability is small	• The control of all vehicular body parts in motion, such as the following: – Continuous activation of lock relay; – Activation of windshield wipers; – Trunk unlocking; – Unlocking doors; – Permanent activation of the 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 ; – Scalability is high.	• Code robustness • Restricted access to OBD port	5	1	1	3	5	3
	S, T, D, E	• Authenticity, Integrity, Availability, and Authorization	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 [114,115] • Practical attack [65,70,79,83,113] • 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	• Code robustness • Restricted access to OBD port	5	1	1	3	5	3
	S, T, D, E	• Authenticity, Integrity, Availability, and Authorization	Electronic Brake Control Module (EBCM)	• Device control packet manipulation using fuzzing and sniffer • Packet sniffing and targeted probing on a car • Access to the CAN bus network • Practical attack [65,70,79] • Scalability is small	• Lock of individual brakes without unlocking EBCM • Engages front left brake • Engages front right brake/unlocks front left brake • Unevenly engages right brakes • Releases brakes, prevents braking	• Code robustness • Restricted access to OBD port	5	1	1	3	5	3
	S, T, D, E	• Authenticity, Integrity, Availability, and Authorization	Autolock feature for doors, trunk, charging port, and fuel lid—passive keyless entry system—key fob [116]	• Replay over the Cable attack: Relay of low-frequency and ultra-high-frequency signals through the generation of magnetic fields to trigger the key fob which demodulates and recovers the original message from the vehicle. Two antennas and an amplifier. Antennas near the door handle capture the beacon signal as a magnetic field locally. This is sent to the other end of the antenna through the amplifier, where it is amplified to increase the signal quality. When this signal reaches the other end, it creates a magnetic field in a second antenna. The PKES would demodulate and message the automobile. • Remote access • Practical attack [65,68,70,79,117–130] • Scalability is high	• Passive keyless entry systems compromised • Vehicle unlocking • Ignition system	• Immediate countermeasures: shielding the key, and removing the battery from the key • Midterm countermeasures: software-only modification, access control restriction, and hardware modification	5	3	3	4	5	4
	E	• Authorization	Autolock doors and trunk—passive keyless entry system—key fob [77]	• Replay over-the-air attack: RF links 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	• Immediate countermeasures: shielding the key, removing the battery from the key • Midterm countermeasures: software-only modification, access control restriction, and hardware modification	5	3	3	4	5	4

Table A4. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
V-TD10: Data Analysis	R, I	• Nonrepudiation, Confidentiality, and Privacy	• Cooperative Awareness Message (CAM) [37]	• Malicious advertisers(V2V/V2I) generate congestion response messages based on the content of the congestion requests [54,60,75,76] • Proximity—remote access [37] • Simulated attack [37] • Scalability is high [37]	• The overall speed of CAVs could be affected. Increase in traffic in the targeted or neighboring roads. Parked bots or compromised vehicles could be infected	• Correlation of messages from neighboring vehicles and cross-verification	5	4	4	5	3	4.2
	T, R, I, E	• Integrity, Nonrepudiation, Confidentiality, Privacy, and Authorization	• Cooperative cruise control module • Localization • Vehicle control warning, e.g., lane departure warning • Vehicle intersection warning • Object identification • Vehicle control automation • Sensor fusion	• Fake env. conditions for camera lens [94] • Inject fabricated frames directly into the 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 changes 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 generates models or alters internal memory with fabricated frames [54,60,75,76] • Inject code to fuse sensed data to indicate warnings and malicious outputs [71,94,105,131]	• Compromised cooperative cruise control functionalities leading to the following: – An accident; – The inability to activate functions; – Driving into traffic; – Discomfort. • The following are the subimpacts: – Sensor information altered; – Sensor preprocessor manipulated; – Main processor manipulated; – Audio system exposed; – HMI is vulnerable; – Low-level controllers influenced; – Vehicle status altered; – Road and environmental condition prediction modules influenced; – Altered video frames, graphic models; – Altered vehicle dynamics information.	• Conserve functional simplicity • Securing real-time analytical software and operating system • Zero-trust architecture • Multi-interface security and isolation [24]	5	4	3	5	4	4.2
V-TD11: Devices and Peripherals	D, E	• Availability and Authorization	• Bluetooth-enabled smartphone devices [77,132] • Company-owned proprietary devices	• Indirect Bluetooth access: vulnerability present in the custom interface code of the Bluetooth-enabled telematics system. This requires pairing an adversarial device to the vehicle's Bluetooth • Direct Bluetooth access: vulnerability present in the custom interface code of the Bluetooth-enabled telematics system. This requires pairing an adversarial device to the vehicle's Bluetooth • Execution of any arbitrary code and taking control of the entire Vehicular systems • Remote access • Physical access [81] • Practical attack [69,80,122,133,134] • 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 the telematics ECU's Unix operating system • Exfiltration of data	• Restrict access	5	3	3	3	3	3.4
	S, T, I	• Authenticity, Integrity, Confidentiality, and Privacy	• User devices (insider, guest, bring-your-own-device for employees) [77] • Mobile applications	• Information injection: device controlled by an adversary can inject malicious code or information [135] • Service manipulation: virtual machines could be manipulated • Information disclosure of vehicles and RSUs [92,112,120,136,137]	• Execution of any arbitrary code and taking control of the entire Vehicular systems by access to program handling Bluetooth functionality • Compromise of the telematics ECU's Unix operating system • Exfiltration of data	• Restrict access • Anomaly detection techniques	3	4	3	3	3	3.2

Table A5. Edge/Cloud and Cloud Threats (Red: High-Risk, Yellow: Medium-Risk, Blue: Low-Risk).

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
E-TD1, C-TD1 Edge/Cloud Communication (Wifi, Cellular, 5G/LTE)	D	• Availability	Wireless communication (WiFi, 5G/LTE)	Denial of Service and distributed DoS by wireless jamming	• Disrupt the vicinity of the impacted network • Channel hopping • Reactive jamming detection techniques, control channel attack prevention • Trigger node identification	Protocols and services can be designed to operate in an autonomous or semiautonomous manner	3	3	3	4	3	3.2
	S, T, I	• Authenticity • Integrity • Confidentiality • Privacy	Wireless Communication Module (WiFi, 5G/LTE)	• Adversaries can launch attacks such as eavesdropping and/or traffic injection • Public network IP [66,78]	Gateway compromised and access to internal network interfaces. Dangerous attack	Jamming detection and prevention techniques, such as the following: • Network segmentation; • The system must check if the access rights of the system have any malicious modifications; • TLS encryption; • RADIUS authentication server.	4	3	1	3	3	2.8
	E	• Authorization	Wireless Communication Module (Wifi, 5G/LTE)	Rogue gateway: open system where any devices can be part of the system	An adversary may gain privileges to propagate the network and create personal cloudlets	The system must check if the access rights of the system have any malicious modifications	5	2	1	4	2	2.4
E-TD2, C-TD3: Microservices	D	• Availability	Wireless communication, virtualization servers	Physical damage: the systems may not be guarded as they may be managed by the service provider	• The impacts of both 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	• Identity management and authentication • Protocol and network security • Code robustness • Restricted access • Distributing services and migrating virtual machines	5	3	2	5	1	3.2
	I	• Confidentiality • Privacy		Privacy leakage: internal threats and honest but curious actors may attempt to access the information [66,78]			4	4	2	4	5	3.8
	E	• Authorization		Privilege escalation: infrastructure could be misconfigured			4	3	2	4	2	3
	T, I	• Integrity • Confidentiality • Privacy		• Service manipulation such as amending the functions of a CAV application such as forming, joining, leaving, merging, splitting, ending, and changing leader • Covert channel attack • Black/gray hole attack			5	2	2	5	2	3.2
E-TD3, C-TD4: API	I	• Confidentiality • Privacy	Local infrastructure interface, vehicle-to-car interfaces	Privacy leakage: internal threats and honest but curious actors may attempt to access the information [66,68,78,104]	• The impacts of both 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	• Identity management and authentication • Protocol and network security • Code robustness • Restricted access	3	4	3	4	5	3.8
	E	• Authorization		Privilege escalation: infrastructure could be misconfigured			4	3	2	4	2	3

Table A5. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
	T, I	• Integrity • Confidentiality • Privacy		Service manipulation such as amending the functions of a CAV application [138]			5	2	2	5	2	3.2
	T, I	• Integrity • Confidentiality • Privacy		Rogue services			5	2	2	5	2	3.2
E-TD4, C-TD7: Physical Input/Outputs	T, R, I, E	• Integrity • Confidentiality • Privacy • Nonrepudiation • Availability • Authorization	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 the edge • Exfiltrate data	• Identity management and authentication • Protocol and network security • Network segmentation • Zero-trust architecture • Code robustness • Restricted access	5	5	4	5	3	4.4
E-TD5, C-TD2: Edge Process and Data Analysis	T, R	• Integrity, Nonrepudiation	Wrong data, protocols and data from communication, microservices, and data storage module [54,75]	• Inject fake env. conditions for edges [94] • 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 generates models or alters internal memory with fabricated frames • Inject code to fuse sensed data to indicate warnings and malicious outputs [81,139,140]	• Midlevel vehicle function optimizer, Local Dynamic Map, security management, edge platform management • The overall information for CAVs could be affected. This can lead to a joint increase in traffic on the targeted or neighboring roads. Parked bots or compromised vehicles could be infected • Leads to traffic • Leads to discomfort	• Correlation of messages from neighboring vehicles and cross-verification • Conserve functional simplicity • Securing real-time analytical software and operating system • Zero-trust architecture • Multi-interface security and isolation [24] • Code robustness and testing	4	3	3	5	3	3.6
E-TD6, C-TD5: Data Storage	T, I	• Integrity • Confidentiality • Privacy	• 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 the 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 [136,141,142] • Replay of frames • Delete/reveal the system software or data [78] • Proximity—remote access [37] • Simulated attack [37,143–150] • Scalability is high [37]	• False warnings or services • Removed warnings or services • Delayed warnings or services	• Correlation of messages from neighboring vehicles and cross-verification • Restrict access and improve code robustness	5	3	3	5	3	3.8
E-TD7, CTD8: Energy System	D	• Availability	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.	• Protect and shield energy system using reflectance techniques with thermal qualities, practices with disaster recovery techniques • If the engagement can be detected, the systems can be protected using electronic warfare weapon • Deployment of attack sensors • Deployment of a surveillance system • Development or maintenance of electronic countermeasures and electro-optical countermeasures	5	5	5	5	5	5

Table A5. *Cont.*

Trust Domain	STRIDE	Security Req.	Entry Point	Threat Desc.	Impact	Countermeasures	D	R	E	A	D	Risk
E-TD8: Actuators	D	• Availability	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	• Code robustness • Restricted access	4	3	2	4	4	3.4
E-TD9, C-TD6: Monitoring	E	• Authorization	White-box and black-box attack	The adversarial model is more effective at producing successful mispredictions of signboards at a quicker pace and with a larger likelihood of failure [111] - Remote access - Theoretical attack - Scalability is high	• Mispredictions of signboards	Intrusion detection system with better machine learning algorithms that could predict images based on the following [94]: - Size; - Angle; - Focus; - Context; - Surface; - Lightning; - Depth.	3	2	3	4	2	2.8
E-TD10: Edge Sensors	S, T, D	• Authenticity • Integrity • Availability	Internal sensors which relies on the network layer [151]	• 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	• Zero-trust architecture • Deperimeterization • Software-defined perimeter	3	3	3	3	2	2.8
	S, T, R, D, E	• Authenticity • Integrity • Nonrepudiation • Availability • Authorization	External sensors include rain sensors, pH sensors, smart meters, temperature sensors, humidity sensors, sound sensors, vibration sensors, chemical sensors, and pressure sensors [151]	• Tampering • Sensor device capture • Fake device and malicious data • Sybil attack • Source device authentication problem • Implicit deduction from sensor behavior • Encryption leakage			4	4	3	4	3	3.4
E-TD11: Devices	T, I	• Integrity • Confidentiality • Privacy	User devices (insider, guest, bring-your-own-device for employees) [77]	• Information injection: device controlled by an adversary can inject malicious code or information [135] • Service manipulation: virtual machines could be manipulated • Information disclosure of vehicles and RSUs [137,141]	• Execution of any arbitrary code and taking control of the entire vehicular systems by access to program handling Bluetooth functionality • Compromise of the telematics ECU's Unix operating system • Exfiltration of data	• Restrict access • Anomaly detection techniques	3	4	3	3	3	3.2
E-TD12: Roadside Infrastructure	E	• Authorization	These devices could be endnotes 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 [81,133,134,139,140,152,153] • Scalability is high	• Execution of any arbitrary code and taking control the systems by access to programs • Compromise the operating system • Exfiltration of data • Analysis of the current contextual awareness	• Restrict access • Anomaly detection techniques	4	4	3	3	4	3.6

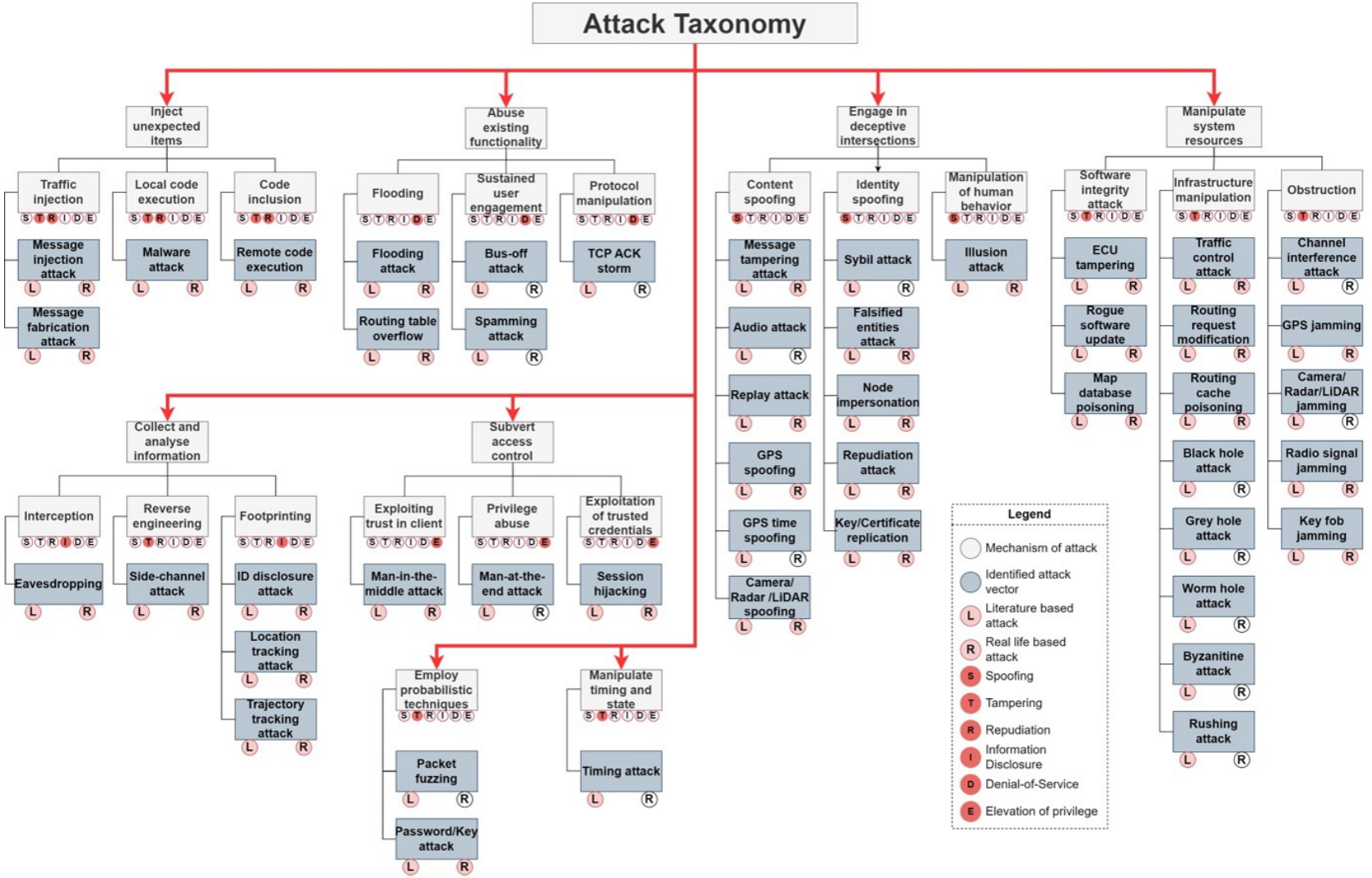

Figure A1. Mapping of documented threats, vulnerabilities, and attacks from the literature and real-world attacks against STRIDE onto a modified attack taxonomy based on CAPEC-1000 attack mechanisms [8,154].

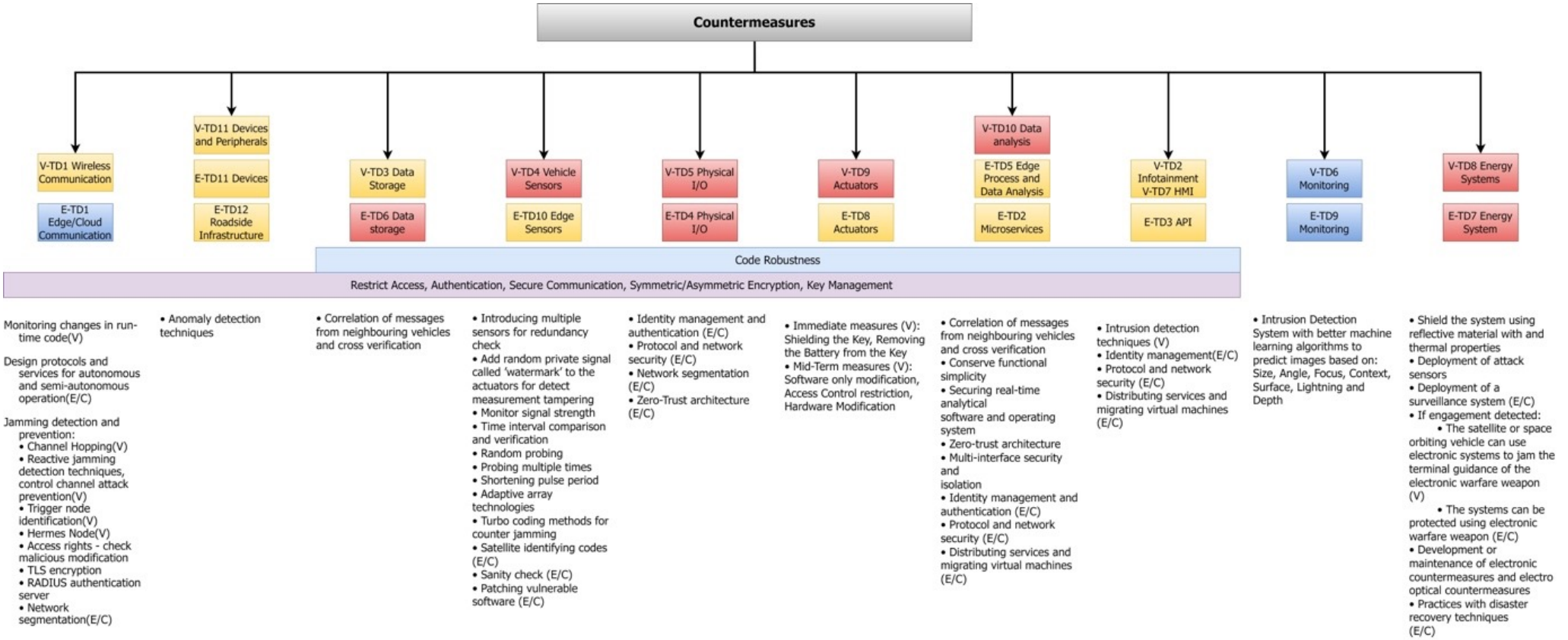

Figure A2. Detailed defense taxonomy for CCAV attack mechanisms.

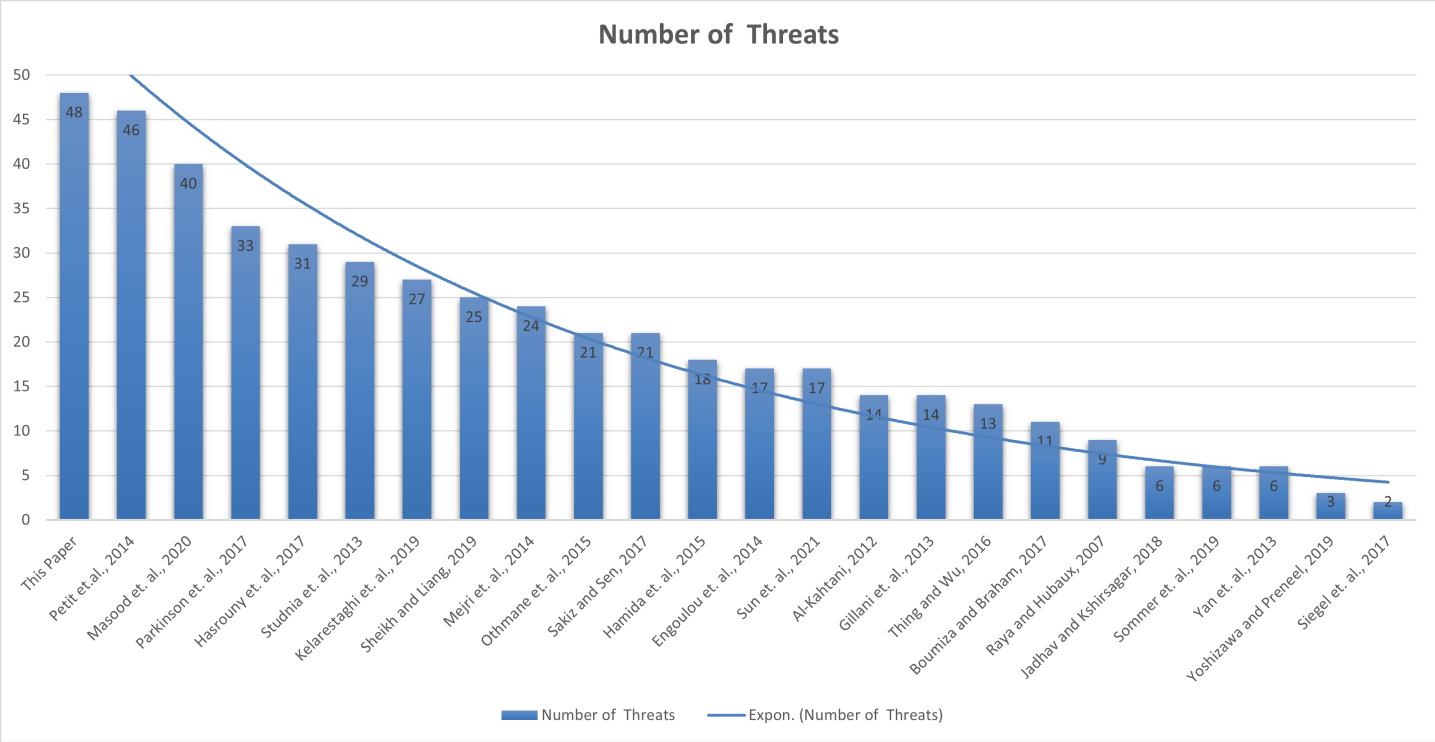

Figure A3. Number of identified threats from the taxonomy against other papers in the literature [3,23,25,27,29,34,39,40,50–64], adapted from [8].

References

1. 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]
2. 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.
3. Sheikh, M.S.; Liang, J. A comprehensive survey on VANET security services in traffic management system. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 2423915. [CrossRef]
4. Maple, C. Security and privacy in the internet of things. *J. Cyber Policy* **2017**, *2*, 155–184. [CrossRef]
5. Maple, C.; Bradbury, M.; Le, A.T.; Ghirardello, K. A connected and autonomous vehicle reference architecture for attack surface analysis. *Appl. Sci.* **2019**, *9*, 5101. [CrossRef]
6. Sheik, A.T.; Atmaca, U.I.; Maple, C.; Epiphaniou, G. Challenges in threat modelling of new space systems: A teleoperation use-case. *Adv. Space Res.* **2022**, *70*, 2208–2226. [CrossRef]
7. HM Government. Connected & Automated Mobility 2025: Realising the Benefits of Self-Driving Vehicles in the UK. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1099173/cam-2025-realising-benefits-self-driving-vehicles.pdf (accessed on 16 October 2023).
8. Sheik, A.T.; Maple, C.; Epiphaniou, G.; Dianati, M. Threat Analysis of Platooning—A Cloud Assisted Connected and Autonomous Vehicle Application. *Information* **2024**, *15*, 14. [CrossRef]
9. Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA , 2014.
10. 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]
11. USDOT. VS15: Infrastructure Enhanced Cooperative Adaptive Cruise Control. Available online: https://www.arc-it.net/html/servicepackages/sp190.html#tab-3 (accessed on 16 October 2023).
12. Xiong, W.; Lagerström, R. Threat modeling—A systematic literature review. *Comput. Secur.* **2019**, *84*, 53–69. [CrossRef]
13. Khan, R.; McLaughlin, K.; Laverty, D.; Sezer, S. STRIDE-based threat modeling for cyber-physical systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 26–29 September 2017; pp. 1–6.
14. Alberts, C.; Behrens, S.; Pethia, R.; Wilson, W. *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0*; Technical Report CMU/SEI-99-TR-017; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 1999.
15. Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C. *Introduction to the OCTAVE Approach*; Technical Report; Carnegie Mellon University Software Engineering Institute: Pittsburgh, PA, USA, 2003.
16. UcedaVelez, T.; Morana, M.M. *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
17. McCarthy, C.; Harnett, K.; Carter, A. *Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach*; Technical Report; National Highway Traffic Safety Administration: Washington, DC, USA, 2014.
18. Lallie, H.S.; Debattista, K.; Bal, J. A review of attack graph and attack tree visual syntax in cyber security. *Comput. Sci. Rev.* **2020**, *35*, 100219. [CrossRef]
19. Committee, S.V.E.S.S. *SAE J3061-Cybersecurity Guidebook for Cyber-Physical Automotive Systems*; SAE—Society of Automotive Engineers: Warrendale, PA, USA, 2016.
20. Jamil, A.M.; Khan, S.; Lee, J.K.; Othmane, L.B. Towards Automated Threat Modeling of Cyber-Physical Systems. In Proceedings of the 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), Pekan, Malaysia, 24–26 August 2021; pp. 614–619.
21. Shevchenko, N.; Frye, B.; Woody, C. *White Paper: Threat Modelling for Cyber-Physical System-of-Systems: Methods Evaluation*; Technical Report; Software Engineering Institute, Carnegie Mellon University: Pittsburgh, PA, USA, 2018.
22. Schneier, B. *Secrets and Lies: Digital Security in a Networked World*; John Wiley & Sons: Hoboken, NJ, USA, 2015.
23. 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.
24. Zhao, M. Advanced driver assistant system, threats, requirements, security solutions. *Intel Labs* **2015**, 2–3.
25. Petit, J.; Shladover, S.E. Potential Cyberattacks on Automated Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2014**, *16*, 546–556. [CrossRef]
26. Miller, C.; Valasek, C. Remote exploitation of an unaltered passenger vehicle. *Black Hat* **2015**, *2015*, 1–91.
27. Hamida, E.; Noura, H.; Znaidi, W. Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. *Electronics* **2015**, *4*, 380–423. [CrossRef]
28. Javed, M.A.; Hamida, E.B.; Znaidi, W. Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. *Sensors* **2016**, *16*, 879. [CrossRef] [PubMed]
29. Sakiz, F.; Sen, S. A survey of attacks and detection mechanisms on intelligent trasnportation system—VANETS and IoV. *Hoc Netw.* **2017**, *61*, 33–50. [CrossRef]

30. Bariah, L.; Shehada, D.; Salahat, E.; Yeun, C.Y. Recent advances in VANET security: A survey. In Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-fall), Boston, MA, USA, 6–9 September 2015; pp. 1–7.
31. 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]
32. La, V.H.; Cavalli, A. Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey. *Int. J. Adhoc Netw. Syst.* **2014**, *4*, 1–20. [CrossRef]
33. Amoozadeh, M.; Raghuramu, A.; Chuah, C.N.; Ghosal, D.; Zhang, H.M.; Rowe, J.; Levitt, K. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [CrossRef]
34. Engoulou, R.G.; Bellaïche, M.; Pierre, S.; Quintero, A. VANET security surveys. *Comput. Commun.* **2014**, *44*, 1–13. [CrossRef]
35. Burt, A. Privacy and cybersecurity are converging. Here's why that matters for people and for companies. *Harv. Bus. Rev.* **2019**, *10*, 1–6.
36. Petit, J.; Feiri, B.S.M.; Kargl, F. Remote Attacks on Automated Vehicles Sensors Experiments on Camera and LiDAR. Experiments on Camera and Lidar. *Black Hat* **2015**, *11*, 995.
37. 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, 8–11 February 2015.
38. National Highway Traffic Safety Administration. *Cybersecurity Best Practices for Modern Vehicles*; Report No. DOT HS; National Highway Traffic Safety Administration: Washington, DC, USA, 2016; Volume 812, pp. 17–20.
39. Mejri, M.N.; Ben-Othman, J.; Hamdi, M. Survey on VANET security challenges and possible cryptographic solutions. *Veh. Commun.* **2014**, *1*, 53–66. [CrossRef]
40. 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.
41. Hubaux, J.P.; Capkun, S.; Jun, L. The security and privacy of smart vehicles. *IEEE Secur. Priv.* **2004**, *2*, 49–55. [CrossRef]
42. Khodaei, M.; Papadimitratos, P. The key to intelligent transportation: Identity and credential management in vehicular communication systems. *IEEE Veh. Technol. Mag.* **2015**, *10*, 63–69. [CrossRef]
43. Eiza, M.H.; Ni, Q. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. *IEEE Veh. Technol. Mag.* **2017**, *12*, 45–51. [CrossRef]
44. Othmane, L.B.; Fernando, R.; Ranchal, R.; Bhargava, B.; Bodden, E. Likelihoods of Threats to Connected Vehicles. *Int. J. Next-Gener. Comput.* **2014**, *5*, 290–303.
45. ABI. Connected Vehicle Cloud Platforms. Available online: https://www.abiresearch.com/market-research/product/1022093-connected-vehicle-cloud-platforms/ (accessed on 16 October 2023).
46. Senior, S.; Rec, C.; Nishar, H.; Horton, T. *AWS Connected Vehicle Solution*; Amazon: Seattle, WA, USA, 2018.
47. Fu, Z.; Hu, W.; Tan, T. Similarity based vehicle trajectory clustering and anomaly detection. In Proceedings of the IEEE International Conference on Image Processing 2005, Genova, Italy, 11–14 September 2005; Volume 2, p. II-602.
48. Mullins, J. Ring of steel II-New York City gets set to replicate London's high-security zone. *IEEE Spectr.* **2006**, *43*, 12–13. [CrossRef]
49. Müter, M.; Groll, A.; Freiling, F.C. A structured approach to anomaly detection for in-vehicle networks. In Proceedings of the 2010 Sixth International Conference on Information Assurance and Security, Atlanta, GA, USA, 23–25 August 2010; pp. 92–98.
50. 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]
51. Raya, M.; Hubaux, J.P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]
52. Al-Kahtani, M.S. Survey on security attacks in vehicular ad hoc networks (VANETs). In Proceedings of the 2012 6th International Conference on Signal Processing and Communication Systems, Gold Coast, QLD, Australia, 12–14 December 2012; pp. 1–9.
53. 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: Berlin/Heidelberg, Germany, 2013; pp. 59–74.
54. 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: Berlin/Heidelberg, Germany, 2015; pp. 217–247.
55. 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]
56. 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*, 1–16. [CrossRef]
57. Hasrouny, H.; Samhat, A.E.; Bassil, C.; Laouiti, A. VANet security challenges and solutions: A survey. *Veh. Commun.* **2017**, *7*, 7–20. [CrossRef]
58. 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.
59. 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.

60. Sommer, F.; Dürrwang, J.; Kriesten, R. Survey and classification of automotive security attacks. *Information* **2019**, *10*, 148. [CrossRef]
61. 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.
62. 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.
63. 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]
64. Sun, X.; Yu, F.R.; Zhang, P. A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6240–6259. [CrossRef]
65. 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 16 October 2023).
66. 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 16 October 2023).
67. 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 16 October 2023).
68. Curry, S. More Car Hacking! Available online: https://twitter.com/samwcyo/status/1597792097175674880 (accessed on 16 October 2023).
69. 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 16 October 2023).
70. 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 16 October 2023).
71. Computest. Car Hack Project Volkswagen/Audi. Available online: https://www.computest.nl/en/knowledge-platform/rd-projects/car-hack/ (accessed on 16 October 2023).
72. Tencent. Tesla Model S Wi-Fi Protocol Stack Vulnerability. Available online: https://v.qq.com/x/page/v304513meir.html (accessed on 16 October 2023).
73. BlackHat. Multiple Vulnerabilities Disclosed in Black Hat VW ID Series. Available online: https://www.blackhat.com/eu-22/ (accessed on 16 October 2023).
74. 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]
75. 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]
76. 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**, 1–53. . [CrossRef]
77. 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), Zürich, Switzerland, 21–25 February 2011; Volume 2011.
78. 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 16 October 2023).
79. 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.
80. Obzy. BMW 330I 2011 Format String DOS Vulnerability(CVE-2017-9212). Available online: https://twitter.com/__obzy__/status/864704956116254720 (accessed on 16 October 2023).
81. CISA. ICS Advisory. Available online: https://nvd.nist.gov/vuln/detail/CVE-2017-9212 (accessed on 16 October 2023).
82. Samcurry. Cracking My Windshield and Earning $10,000 on the Tesla Bug Bounty Program. Available online: https://bit.ly/3XXgJFC (accessed on 16 October 2023).
83. 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 16 October 2023).
84. NIST. CVE-2020-28656 Detail. Available online: https://nvd.nist.gov/vuln/detail/CVE-2020-28656 (accessed on 16 October 2023).
85. Tencent. Tencent Security Keen Lab: Experimental Security Assessment of Mercedes-Benz Cars. Available online: https://bit.ly/3R7TBlD (accessed on 16 October 2023).
86. 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 16 October 2023).
87. 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 16 October 2023).
88. Keen Security Lab. Experimental Security Assessment of BMW Cars by KeenLab. Available online: https://bit.ly/34ICOBC (accessed on 16 October 2023).
89. Keen Security Lab. Tencent Security Keen Lab: Experimental Security Assessment of Mercedes-Benz Cars. Available online: https://bit.ly/34Gpqhj (accessed on 16 October 2023).

90. 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, 8–12 August 2011.
91. Sgayou. Subaru Starlink Persistent Root Code Execution. Available online: https://github.com/sgayou/subaru-starlink-research (accessed on 16 October 2023).
92. 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 16 October 2023).
93. Zehavi, I.; Shamir, A. Facial Misrecognition Systems: Simple Weight Manipulations Force DNNs to Err Only on Specific Persons. *arXiv* **2023**, arXiv:2301.03118.
94. Nassi, B.; Nassi, D.; Ben-Netanel, R.; Mirsky, Y.; Drokin, O.; Elovici, Y. Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems. 2020. Available online: https://eprint.iacr.org/2020/085 (accessed on 16 October 2023).
95. Yan, C.; Xu, W.; Liu, J. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def. Con.* **2016**, *24*, 109.
96. 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]
97. 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]
98. Pham, M.; Xiong, K. A survey on security attacks and defense techniques for connected and autonomous vehicles. *Comput. Secur.* **2021**, *109*, 102269. [CrossRef]
99. Mukhopadhyay, M.; Sarkar, B.; Chakraborty, A. Augmentation of anti-jam GPS system using smart antenna with a simple DOA estimation algorithm. *Prog. Electromagn. Res.* **2007**, *67*, 231–249. [CrossRef]
100. Purwar, A.; Joshi, D.; Chaubey, V.K. GPS signal jamming and anti-jamming strategy—A theoretical analysis. In Proceedings of the 2016 IEEE Annual India Conference (INDICON), Bangalore, India, 16–18 December 2016; pp. 1–6.
101. 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]
102. 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.
103. 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 16 October 2023).
104. Bitsight. Bitsight Discovers Critical Vulnerabilities in Widely Used Vehicle GPS Tracker. Available online: https://bit.ly/3je70fd (accessed on 16 October 2023).
105. 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 16 October 2023).
106. Warner, J.S.; Johnston, R.G. GPS spoofing countermeasures. *Homel. Secur. J.* **2003**, *25*, 19–27.
107. Mitre. CVE-2020-15912. Available online: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15912 (accessed on 16 October 2023).
108. 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, Washington, DC, USA, 10–11 August 2015.
109. Burakova, Y.; Hass, B.; Millar, L.; Weimerskirch, A. Truck Hacking: An Experimental Analysis of the SAE J1939 Standard. *WOOT* **2016**, *16*, 211–220.
110. 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.
111. 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.
112. 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 16 October 2023).
113. Tencent. Tencent Keen Security Lab: Experimental Security Assessment on Lexus Cars. Available online: https://bit.ly/3XIZhos (accessed on 16 October 2023).
114. 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]
115. Smith, C. *2014 Car Hackers Handbook-Open Garages*; Theia Labs: Waterloo, ON, Canada, 2014.
116. 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 August 2013; pp. 703–718.
117. 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 16 October 2023).
118. 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 16 October 2023).

119. 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 16 October 2023).
120. 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 16 October 2023).
121. Kunnamon. Redacted TBONE Document Submitted to Tesla Bug Bounty Program. Available online: https://kunnamon.io/tbone/ (accessed on 16 October 2023).
122. John, D. Canadian Software Developer Discovers Bluetooth Key Vulnerability That Allows Anyone to Unlock a Tesla. Available online: https://bit.ly/408iH88 (accessed on 16 October 2023).
123. HackingIntoYourHeart. Unoriginal Rice Patty is My Personal Title for the Replay-Based Attack on Honda and Acura Vehicles. Available online: https://github.com/HackingIntoYourHeart/Unoriginal-Rice-Patty (accessed on 16 October 2023).
124. ReverseKevin. Honda Civic Replay Attack. Available online: https://www.youtube.com/watch?v=NjbjepeILrk (accessed on 16 October 2023).
125. 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 16 October 2023).
126. 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 16 October 2023).
127. Khan, S. Technical Advisory—Tesla Ble Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks. Available online: https://bit.ly/3DiuZ3M (accessed on 16 October 2023).
128. Trifinite. Project Tempa. Available online: https://trifinite.org/stuff/project_tempa/ (accessed on 16 October 2023).
129. Rollingpwn. Rolling PWN Attack. Available online: https://rollingpwn.github.io/rolling-pwn/ (accessed on 16 October 2023).
130. 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 16 October 2023).
131. 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 16 October 2023).
132. 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.
133. VDECert. SWARCO: Critical Vulnerability in CPU LS4000. Available online: https://cert.vde.com/de/advisories/VDE-2020-016/ (accessed on 16 October 2023).
134. 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 16 October 2023).
135. 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]
136. Whittaker, Z. Mercedes-Benz App Glitch Exposed Car Owners' Information to Other Users. Available online: https://bit.ly/3HdD7Uh (accessed on 16 October 2023).
137. 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 16 October 2023).
138. 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 16 October 2023).
139. Schneider. Schneider Electric Security Notification. Available online: https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-194-06 (accessed on 16 October 2023).
140. XiunoBBS. Vulnerability Mining Practice of Charging Piles. Available online: https://bbs.kanxue.com/thread-272546.htm (accessed on 16 October 2023).
141. Di, W. Information on 100,000 Citroen Owners May Have Been Leaked. Available online: shorturl.at/beSTV (accessed on 16 October 2023).
142. 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 16 October 2023).
143. 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 16 October 2023).
144. 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 16 October 2023).
145. MBUSA. Mercedes-Benz USA Announces Initial Findings of Data Investigation Affecting Customers and Interested Buyers. Available online: https://bit.ly/3wS6Hu5 (accessed on 16 October 2023).
146. 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 16 October 2023).
147. 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 16 October 2023).

148. 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 16 October 2023).
149. Redazione. La Ferrari è Stata Colpita Dal Ransomware Ransomexx. 7GB di Dati Scaricabili Online. Available online: https://www.redhotcyber.com/post/la-ferrari-e-stata-colpita-dal-ransomware-ransomexx-7gb-di (accessed on 16 October 2023).
150. Nio. Statement on Data Security Incidents. Available online: https://app.nio.com/app/web/v2/share_comment?id=2284166&type=essay (accessed on 16 October 2023).
151. 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]
152. 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 16 October 2023).
153. Eckert, S. Replay Attack: Numerous Traffic Lights in Germany are Vulnerable to Manipulation. Available online: https://twitter.com/sveckert/status/1600443031915663360 (accessed on 16 October 2023).
154. Pekaric, I.; Sauerwein, C.; Haselwanter, S.; Felderer, M. A taxonomy of attack mechanisms in the automotive domain. *Comput. Stand. Interfaces* **2021**, *78*, 103539. [CrossRef]