Key Security Challenges for Cloud-Assisted Connected and Autonomous Vehicles

Al Tariq Sheik[1], Carsten Maple[2]

[1]Doctoral Researcher, WMG, University of Warwick, CV4 7AL, Coventry, UK
[2]Professor of Cyber Systems Engineering, University of Warwick. CV4 7AL, Coventry, UK
t.sheik@warwick.ac.uk, cm@warwick.ac.uk

Keywords: CONNECTED AND AUTONOMOUS VEHICLES, CLOUD, ATTACK TAXONOMY, ADAPTIVE SECURITY

Abstract

Connected and Autonomous Vehicles (CAVs) bring situational awareness to vehicles promising a safer transportation system. To support collaborative awareness, cloud-assisted CAV are being developed besides Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. CAVs require efficient and accurate information from numerous sources, internal and external to the vehicle, for time-critical safety applications. As such, cloud-assisted CAVs would be exposed to a large amount of dynamic information (such as speed, location, vehicle ID, travel routes, passengers' personal information, bank details and so on). Moreover, CAVs have a reasonably long lifetime due to which the associated vehicular technologies in CAVs age and it is possible that vulnerabilities can be exploited to inflict harm. As a result, when technologies change, the security requirements evolve. This research aims to discuss significant research challenges, classify emerging threats, attacks and countermeasures and identify immediate research directions to protect the evolving cloud-assisted CAVs with security mechanisms to adapt to complex and dynamic environments.

1. Introduction

The Internet of Things (IoT) is advancing, and interest in connecting Autonomous Vehicles (AVs) is increasing despite the continuously evolving cyber threats. The automotive industry and government departments are harnessing the potential of Connected Autonomous Vehicles' (CAVs) to develop safe, secure, sustainable, and intelligent vehicles. Examples include Tesla who have recorded more than 4 billion miles of vehicle data, far outweighing Google's Waymo which had logged more than 3 million miles in 2017 [1-3]. In 2020, according to Habeck, et al. [4], global annual revenue from connected vehicle services alone is expected to be EUR 170 – 180 billion envisioning features and applications with different on-board vehicular connections by 2025. This represents a six-fold increase from approximately EUR 30 billion in 2014. This economic benefit is supplemented by the aim of ensuring safety by reducing accidents, improving traffic and personalised on-board entertainment through CAV applications (such as fleet management, vehicle platooning, localised weather and so on). Furthermore, with the advancements in electric and hybrid vehicle technologies, CAVs are expected to emit less pollution compared to traditional vehicle, thereby benefitting the environment. The advantages of such grandiose CAV predictions are driving the automobile industry to research into developing safe and secure collaborative cloud-assisted CAVs.

Messages such as Cooperative Awareness Messages (CAM) or Basic Safety Messages (BSM) are being designed for vehicular communication. The key communication technologies for sharing these messages are Dedicated Short Range Communication (DSRC) and IEEE 802.11p [5]. In addition, for direct communication to cloud infrastructures, 4G/LTE and 5G technologies are being researched and developed to offer high-speed connectivity for vehicles. CAVs with these external connections can execute numerous applications such as driver assistance and traffic. For these developments, low latency message transmission is considered to be ideal. However, satisfying security requirements while proactively defending against evolving cyber-threats and maintaining the vehicle's operational reliability and safety is a growing concern.

CAVs and Road Side Units (RSUs) will receive, process and transmit vehicular message that are mobile and stationary respectively. These communication nodes can be targeted by motivated adversaries. Since the nodes are distributed across different geographical locations in a connected ecosystem the likelihood of vulnerabilities from remote attacks increases. These attacks are shown to be feasible and have been demonstrated in experiments on vehicles [6, 7]. Distributed Denial of Service (DDOS), Spoofing, Information Disclosure, Elevation of Privileges, Tampering are some of the well-known techniques to manipulate a vulnerable system. Given the fact that CAVs require sophisticated computerised on-board systems, pathways for vulnerabilities may increase through the extended attack surfaces. As recommended by J3061standards, security requirements are to be considered from the design phase for vehicular networks [8]. This includes satisfying security conditions such as Confidentiality, Integrity, Auditability, Safety, Authenticity and Availability and Trustworthiness. Nevertheless, current security practices have been proved to have failed in adhering to crucial security requirements. Therefore, iterative security measures are highly required and the latest developments in monitoring and detection of evolving malicious data remain a major research challenge.

Another concern is that CAV applications require seamless connectivity with optimal utilisation of limited on-board computational resources and security introduces message overheads and time delays. Traditional or static security for CAVs poses a challenging problem for efficient message transmission, reception and computation. This problem is further aggravated when considering the evolving nature of cloud-assisted CAV applications. To resolve this, security mechanisms may have to adapt according to the application and security requirements based on the availability of the resources.

In fact, different vehicular applications require different time and computational resources to process and disseminate information accurately, efficiently and securely. The problem of securing these heterogeneous applications is further exacerbated by the fact that different OEMs and service providers practise different implementations of the same application. To address the problem, industries and governments in the US and Europe have started collaborating to unravel the concerns regarding standardisation, types of technology, policies and adherence to security requirements. However, these collaborations are at an early stage where industries and governments need to work in parallel to regulate and mitigate cyber security risks.

Therefore, this paper identifies significant security challenges for CAVs, and investigates the ways security could be optimally introduced for cloud-assisted CAVs. The objective of this research is to create a taxonomy of attacks and countermeasures that can be used to analyse current threats, approaches and solutions. Using this taxonomy, the article presents the key emerging research directions to ensure the security requirements, Thus, we provide a guide for industry and academics to investigate the domain, and further extend research for cloud-assisted CAVs. This would allow for a safer Internet-of-Vehicles and a more reliable Intelligent Transportation System overall.

To achieve this goal, we first conducted a literature review to determine the array of cyber threats to vehicles. Secondly, a threat analysis is performed through building an attack taxonomy. We then analyse the taxonomy to produce a discussion based the countermeasures and provide a foundation for future research directions.

The remainder of this paper is organised as follows. Section 2 highlights the security requirements and section 3 discusses the key security challenges. Section 4 discusses the ways these challenges could be addressed. Section 5 examines the immediate research direction, before section 6 concludes the study and raises questions for future investigation.

2. Security Requirements

CAVs can be exposed to various threats when interacting with connected infrastructures. The growing number of Electronic Control Units (ECUs), sensors and actuators accounting for data processing and timely decision-making operations makes the issue more problematic. The issue becomes critical in cases where the data impacts vital safety-critical operation. Stringent security requirements are necessary to help ensure the CAV systems are protected from being compromised. Traditional security requirements such as the CIA triad and Parkerian Hexad are ubiquitous but were not designed for CAVs. Therefore, it is important that these security requirements should be revised when designing a security framework for cloud-assisted CAVs. In addition to the traditional security requirements, ensuring vehicle safety is also an added challenge; in CAV environments security and safety requirements overlap and we explore this issue further in Section 3.1. For our study, privacy requirements are excluded from consideration. Thus, following sub-sections discusses the key immediate security requirements for cloud-assisted CAVs [5, 9-11]:

2.1. *Confidentiality*

Vehicular communication systems should protect data when at rest or transit. Appropriate confidentiality measures prevent disclosure of sensitive information to malicious parties. Maintaining data confidentiality requires encryption mechanisms, which in a resource-constrained CAV system may challenge latency-sensitive applications. As such, all communications require consideration of appropriate encryption Perfect Forward Secrecy and ensuring access to any information is through trusted parties.

2.2. *Integrity*

Each cloud-assisted CAVs network systems must be isolated and hardened by applied technology (hardware or software) to minimise risk through frequent auditing, upgrades and patches. Preventative approaches using firewalls, Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) can be implemented to restrict, monitor and protect sensitive information from unauthorised alteration, manipulation or deletion of data. Some of the attacks that could compromise data integrity include masquerading attack, replay attack, message tampering or fabrication and illusion attack.

2.3. *Availability*

In an interconnected ecosystem, there is a wealth of information exchanged across endpoints in real-time (sensors, ECUs, Edge Cloud and so on). Although data reliance, transmission and external connectivity for CAVs are at early stages of development, it is vital to tolerate communication and system downtimes or overcome disruptions (eg: system update) through solutions such as redundant or backup system implementations. Such solutions can be based on anomaly detection, predictable performance and latencies to help the system make a smooth transition or enter into self-governance in case of emergencies. However, managing such downtime must be carefully considered and remains a challenge.

There are different attacks compromising availability of a connected infrastructure which include Denial of Service attack (DOS), jamming attack, greedy behaviour attack, blackhole attack, greyhole attack, sinkhole attack, wormhole attack, broadcast tampering attack, malware attack and spamming attack.

2.4. Authenticity and Trustworthiness

Distinguishing trusted messages from malicious messages is a vital process for CAVs. The ecosystem must be able to authenticate and process valid messages and discard invalid or expired messages by determining the relevance of the message. This is a particularly important security requirement as identification of information source is essential to trust a message for safety-critical applications. Unfortunately, tunnelling attacks, node impersonation attack, GPS spoofing attack and Sybil attacks may violate an authenticity of a system.

2.5. Auditability

Cloud-assisted CAVs share critical messages that may prompt an action. These messages that are processed should be auditable to be held accountable and non-repudiate in case of an investigation. The system should also be able to provide convincing evidence to a vehicles' or entities' interaction. This helps to trace message sources and actions so that nodes do not deny/list false message transmission. To achieve this, each entity should be designed with unique IDs with robust data logging functions to record each reception, transmission and action. Written logs are to be maintained so that each process is time-stamped and can be forensically auditable.

2.6. Safety

There is a unique security requirement for CAV systems as failure of any above-mentioned security requirements may lead to a serious safety concern. CAVs must ensure the protection of life, environment and surroundings. It should be able to prioritise safety of human being irrespective of the decision it makes. On detection of a hazardous situation, the system should position itself to emergency state overriding remote instructions. One way is to adopt trustworthiness to safety-critical algorithms and ensure graceful transition to safe state.

3. Security Challenges

To deliver the future mobility, a connected automotive ecosystem comprises numerous components. Robust road side units, edge computing capabilities, vehicle computation capabilities, communication system and various new developments are required to facilitate the complete autonomy of cloud-assisted CAVs. However, security challenges, liabilities and standardisation hamper the implementation of Intelligent Transportation System (ITS). Secure lifecycle management (see Table 1) is a major consideration for the analysis of security requirements for vehicular applications.

The security over the lifecycle can be summarised as starting, running and staying secure [10]. With respect to security challenges, an example for protecting CAVs involves securing the sensing module, actuation module, and internal processing modules of a vehicle [10]. The sensing and actuator modules should be able to accurately sense and execute commands of the sensed data by tolerating unexpected anomalies by ensuring integrity, availability, authenticity and auditability. To be more precise the internal processing module must be able to ensure [10]:

- Availability of information
- Prevent delays
- Authenticity
- Integrity
- Correct data formats (syntax)
- Accurate correlation of multiple data streams.

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

Table 1: Security Lifecyle of CAV

Discrete embedded system such as those above have a number of different requirements. Applying on-board security for CAVS alone puts forward numerous challenges. External CAV communication with edge-cloud and cloud technologies further extends the attack surface.

The following sub-sections discuss the most significant challenges for securing cloud-assisted CAVs. Of course, there exists a variety of other challenges to implement the cloud-assisted CAVs, such big data, complex supply chains and so on. However, a significant step towards securing cloud-assisted CAV ecosystem would be to incorporate "Security by Design" practices. This paper puts forward three vital challenges that require consideration from the initial design phase that should be addressed in collaboration with governments and automotive industries for integrating cloud technology and CAVs.

3.1. Increased connectivity and evolving characteristics of cloud-assisted CAVs

Developments in the field of V2V and V2I communications are positive and encouraging. Emerging wireless communication technologies enable vehicles to transmit messages for coordinating and manoeuvring in highways and urban scenarios. The information shared between vehicles aims to reduce traffic and to increase safety. Current research aims to deploy DSRC, a development of WAVE (IEEE 802.11p) as a common V2V communication medium.

Another essential component is RSUs for V2I communication. RSUs can communicate with the external network (cloud, edge-cloud, Internet and so on) through broadcasting or exchanging traffic rich information. Also, RSUs can relay the latest information about the locality such as weather and entertainment. The dynamic traffic information (speed, acceleration, location) of each vehicle on the road can be processed in a centralised cloud infrastructure [5, 12, 13]. This capability enables CAVs to make well-informed decisions to choose not only optimal routes with regular updates, but also a variety of application-tailored decisions.

RSUs have a higher communication bandwidth than V2V communication and can be exposed to attacks as they are publicly stationed compared to mobile CAVs. Due to a substantial number of connections needing to be handled by RSUs, challenges such as the ability to detect and differentiate unreliable connections are introduced [14].The characteristics of such a connected ecosystem with increasing complexities raises security concerns. Table 2 gives an overview characteristic of the cloud-assisted CAV ecosystem which introduces various security threats and concerns [5, 14]. As previously stated, it is important that the challenges mentioned in Table 3 are resolved in order to meet the security requirements mentioned in Section 2.

Characteristics	Description
Connected Infrastructure	
Heterogeneous size	Cloud services are envisioned to cater the individual and varying groups of CAVs across several geographical regions
Large scale and unbounded network	Urban and rural areas including highways are to be connected across the nation. The network should be highly scalable and unbounded.
Dynamic network topology	CAVs' mobility and change in network can lead to wireless interference, disconnections and inability to ensure reliable communication handshakes challenging accurate and timely information for vehicular awareness.
Energy, computation power and real-time support	Connected infrastructures have sophisticated power or computational capabilities and should ensure high availability and reliability for CAVs in order to provide real-time updates so that security overheads would not be challenging..
Communication	Regular communication of data packets will be through discrete and hybrid wireless communication channels such as DSRC, WAVE, IEEE 802.11p, 5G, 4G LTE
Physical protection	RSUs would be installed with state-of-the-art technologies to support CAVs. So physical protection of RSU is necessary to prevent adversaries from tampering any components of the infrastructure
Predictability	Cloud services would disseminate updates for CAVs. To do so, the infrastructure units are to learn the changing environment by collecting periodic updates which includes road signs, lanes, traffic signals and congestions. Through this data analysis, additional information may be extracted to predict upcoming events, accidents, failures, traffic etc.
Edge-cloud and Cloud capabilities	Cloud infrastructures can execute remote functions facilitating computation of resource-intensive tasks providing eventful intelligence and overall traffic and vehicle management whereas, edge cloud services could provide localised value-added services for CAVs with regular traffic updates The interconnectivity between the CAV, edge cloud and core cloud introduces a three-tier architecture.
On-board CAV	
Optimal processing requirements for CAV	Different CAV models may contain different capabilities which should adhere to standards and be capable of processing messages through techniques such as adaptive or selective scheduling
Authenticity and trustworthiness	CAVs should ensure integrity and authenticity of messages by registering credentials with a Trusted Authority (TA). The trustworthiness is gained through time period, connectivity duration, history of message and CAV operation.
Message Broadcast	CAV can broadcast periodic messages Notifying the neighbouring vehicles of its whereabouts. This message would contain information about vehicle dynamics such as location, velocity, acceleration and yaw rate etc.

Table 2: Characteristics of cloud-assisted CAVs:

3.2. Integrating Cyber Security into Vehicle Safety Consideration

Vehicles operate with numerous safety systems to protect the driver and passengers. According to SAE J3061 [8], a system is safe when the vehicle's state does not inflict any harm on life, property or the environment whereas a system is secure when the vehicle's state does not allow a vulnerability to be exploited by an adversary inflicting damage to the CAVs safety systems, operations, company's finance and reputation. Both processes demonstrate similar properties such as threat analysis and hazard analysis respectively. However, these processes are so distinct that they require different expertise, resources and practices. An example of critical safety failure is the lack of Uber vehicles ability to detect pedestrians[15]

Security vulnerabilities can compromise safety goals, but the converse is not true. Table 3 explains the similarities, uniqueness and challenges faced by cyber security in vehicles. For example, if erroneous, unverified or malicious data is to be processed by CAVs, it may lead to system decisions that can jeopardise or harm human life. Therefore, it is vital that such systems prioritise safety through anomaly detection, balancing inconsistent data and overcoming erroneous data without hindering the safety functions of the system. This ability to recover is a significant challenge since CAVs are to detect and mitigate anomalies by developing confidence in its decisions despite conflicting data[16, 17]. Such a challenge can be resolved by adopting a system that relies on trust and consensus [18]. It is worth noting that both safety and security processes for CAVs require a synchronised and coordinated approach, and currently, there is a lack of research to execute the processes systematically from the design phase to the testing phase. Another outcome of this convergence helps meet the safety and security requirement mentioned in Section 2.

	Safety	Cyber Security
Similarities	**Safety by Design**	**Security by Design**
	Hazard Analysis and Risk Assessment are conducted safety goals	Threat analysis and risk assessment aiming to meet security goals
	System Requirement: Safety goals	System Requirement: Security goals
	System Design identifies highest risk hazards to eliminate the potential hazards,	System Requirement: high risk identified to help reduce the likelihood of a successful attack.
	System Design: safety goals	System Requirement: Security goals
Uniqueness	Addresses potential hazards through safety mechanism	Addresses potential threats through counter measures
	No adversarial analysis required	Adversarial analysis is required through studying capability
	A system safety-oriented focus	A broad focus
Challenges	➢ Cybersecurity risks continue to change as adversarial capabilities evolve. ➢ Countermeasures may not be evolving and be robust during vehicle system design creation. ➢ Conflict of cyber security and safety could arise during systems requirements and integration.	

Table 3: Similarities, uniqueness and challenges of Vehicular Safety vs Security[8]

3.3. Emerging On-board and Remote Attacks

L3Pilot is a European project aiming to perform large-scale piloting of SAE Level 3 and Level 4 autonomous vehicles. The project has considered the attack taxonomy described in Table 4. The taxonomy aims to determine the possible threats to understand the emerging vulnerabilities from the on-board network through hardware components to long range and short-range external communication. The security of vehicles is of paramount importance, so it is vital that the threats are understood systematically. Table 4 raises questions on the kind of taxonomy that is used for vehicles and the attacks that are considered [5, 9, 19]:

- Sniffing
- Data modification
- Replay
- Masquerading
- Sybil
- Wormhole
- Distributed Denial of Service
- Traffic analysis attack
- Tunnelling
- Spamming
- GPS spoofing
- Denial-of-Service
- Man-in the Middle
- Brute Force Attack
- Illusion attack
- Jamming
- Black Hole
- Misbehaviour Attack
- Bogus Information Attack
- Sink Hole
- Selective forwarding
- Purposeful Attack
- Timing Attack
- Malware

According to Yampolskiy [20], an attack must be understood from the different taxonomic dimensions categorising them into targets, elements, and attacks which are related to each other. Moreover, a systematic taxonomy helps determine security requirements that can ensure reliable operation of the CAV. Therefore, a taxonomy sets an initial step towards threat modelling and identifying different methodologies to protect a system from evolving threats [5, 21].

Cyber-attacks on vehicles can lead to catastrophic impacts. Koscher, et al. [7] demonstrated numerous attacks using a custom developed program, CARSHARK, to attack an on-board ECU and influence a broad array of safety-critical systems. Similarly, Checkoway, et al. [22] injected malicious code into the telematics and infotainment system to demonstrate the ability to send custom commands on the CAN bus to actuate on-board systems. Furthermore, Miller and Valasek [6] successfully compromised a Ford Escape and Toyota Prius, demonstrating remote control of all functionalities of the vehicles while in motion. They built a framework to monitor and demonstrate vehicular vulnerabilities aiming to secure ECU's and the CAN bus network by detection and prevention methods. Similarly, Kamkar [23] developed a hacking tool named Ownstar which could locate, unlock and remote start any vehicle with General Motor's (GM's) OnStar Remote Link after intercepting communications between the Remote Link mobile app and OnStar servers.

Amoozadeh, et al. [24] studies security attacks from the application and network layer on connected vehicles equipped with Cooperative Adaptive Cruise Control (CACC). For a connected ecosystem, since vehicles can communicate with each other through periodically broadcasting messages, containing information such as vehicle position, speed and acceleration, there is vital need to protect this information from being misused. As a countermeasure, misbehaviour or anomaly detection techniques or installation of tamper-proof hardware is a viable solution to detect and flag malicious packets.

4. Addressing Security Challenges

According to standards, threat analysis and risk assessment approaches are proposed for the identification and protection of critical assets [8]. This would involve combining threats from the physical, network, facilities, application and management layer of the CAV architecture [5]. This helps to realise the likelihood of the attack considering the practicality and feasibility by introducing appropriate countermeasures. This section mainly discusses two immediate challenges to be addressed i.e liability and respective security countermeasures.

Liability is one of the major barriers for acceptance of CAVs. There are many issues to be answered even with perfect driving conditions of CAVs: 1) If a CAV is vulnerable to a successful attack, can the vehicle be influenced to cause an accident? 2) How does the vehicle account for its action if it impacts the neighbouring vehicles or pedestrians? 3) Are human-drivers responsible for the split second of decision making? 4)With a large number of sensing and security algorithms being executed, how can an abnormally behaving vehicle prove that it is not a mistake of the vehicle rather than an influence from external sources? [25, 26]

In addition to this, other philosophical questions may be raised to hold accountability of the vehicle's actions. There have been some work to clarify liability concerns[27]; however, there is lack of appropriate standards for liability and security. The following sub section describes how liability and security countermeasures could be resolved.

4.1. Liability – following standards, sharing information

Accountability, the legal obligation of a person or a system to another entity is a method to "give account of, explain and justify actions or decision in an appropriate way" [28]. Accountability can be argued on three categories.

- Standards: To maintain a level of uniformity for CAVs and ITS, standards should be introduced based on documented by governing body. In the case of ITS, it could be the manufacturers following the standards which comply with constitutional laws and legal obligations. Key standards include IEEE, ETSI, SAE, NIST, GDPR,
- Information sharing: The driver/passenger, when utilising a CAV, is made aware of the systems and data processing being on par with the standards and the liability.
- Impose: The driver/passenger has the right of imposing sanction in case a system fails to operate in the manner it was promised to.

Considering the conditions, there is a requirement for robust standards to abide by. However, proving accountability and accruing compensation in case of system failures or accidents is a key research area. There are particularly four scenarios that currently consider the liability issues. From the perspective of Level 3 and Level 4 CAVs, Gurney [26] argues about the liability applying it to a driver who is:

- distracted
- of limited capabilities (old age)
- disabled
- attentive and can drive

Considering the drivers ability, Gurney [26] suggests that CAVs should be completely liable if it is manoeuvring in a Level 4 autonomous mode whereby the driver has least interaction. If not, the attentive drivers should be held accountable for accidents considering the nature of the situation. There are many drawbacks in case of safety. Many critical situations may arise where by a CAV system should be able to determine the liability autonomously by following several steps. Based on the patent, Figure 1 illustrates how a vehicle could determine a liability for a vehicle accident [29]. Similarly, in the case of CAVs, systems should be installed with facilities to determine a liability score. This further requires a segregation of data ownership, particularly entering the 3-tier architecture.

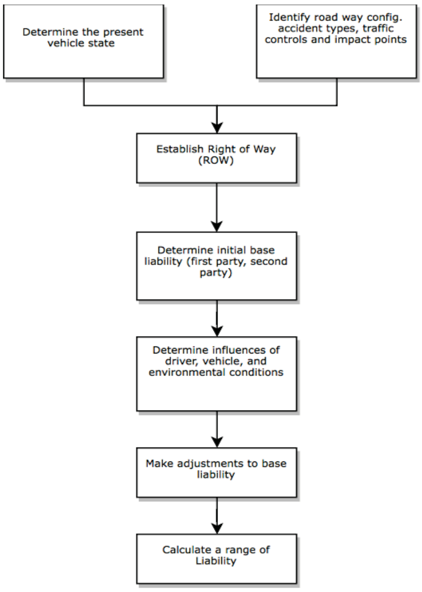
Determine the present vehicle state
Identify road way config. accident types, traffic controls and impact points
Establish Right of Way (ROW)
Determine initial base liability (first party, second party)
Determine influences of driver, vehicle, and environmental conditions
Make adjustments to base liability
Calculate a range of Liability

Figure 1: Computation of liability (first party/ second party) in case of an accident

4.2. Security and Countermeasures

Secure methods adopting different encryption and authentication mechanisms have been proposed by number of standards for CAV and ITS system to protect the ecosystem. Implementing these methods in a cloud-assisted CAV ecosystem is challenging due to the limited computational power in a complex embedded system environment available on-board [30]. The complexity is further magnified when vehicles employ multiple hardware and software from different OEMs. Therefore, relying on a single static security mechanism is not feasible which necessitates multiple security mechanisms for on-board and wireless security. Some of the recent research relies on short term certificates, pseudonyms and efficient revocation list using TA and Public Key Infrastructures (PKI) leveraging RSU [31, 32].

To overcome security vulnerabilities in manufactured vehicles, Over The Air (OTA) software updates were proposed to upgrade and fix software vulnerabilities. Although, introducing OTA updates provides a temporary solution for existing on-board vulnerabilities; the threat of executing malicious code through OTA updates enables adversaries to develop wireless attacks such as code injection or malware attacks if the system is not securely implemented [33].

Alternatively, centralised cloud-based security solutions have been recently discussed by multiple companies such as HERE, Ericsson, IBM, CloudCar, GM OnStar, Amazon AWS etc [34]. Amazon AWS and Ericsson have proposed their respective connected vehicle cloud system architecture where anomaly detection mechanism is widely emphasised in the cloud infrastructure to detect malicious data packets. This mechanism relies on application security mechanism where machine learning algorithms could detect anomalies which is then marked and stored in the local database and to notify the vehicles [33, 35]. This is indeed a development of a broad array of researches that were conducted in the past using vehicle trajectory clustering and entropy-based attack detection mechanism for in-vehicle networks that is being extended to cloud-based security [16, 17, 36].

Similarly, Miller and Valasek [6] assert that automobiles are designed prioritising safety in mind and recommend defensive technologies such as an Intrusion Detection System (IDS) to prevent the attacks on the CAN bus. To detect an attack, mechanism for histogram analysis of diagnostic packets during CAN bus operation could study the repetitive nature of system messages and detect anomalies that indicate deviation from normal operation. Moreover, the National Highway Traffic Safety Administration [37] has proposed a layered approach to harden vehicles electronics by adopting preventive measures through isolation of safety critical and identification systems, intrusion detection and real time response of potential threats and, regular assessment of system thorough solutions shared with information collaboration of past security threats between partners and organisations.

The sooner industries and governments collaborate to resolve liability and cyber security issues the more certainty insurance agencies would have and hence customer scepticism would decrease, and acceptance would increase.

5. Research Directions

The literature review identifies significant studies covering vehicular security such as data authentication and message trustworthiness. Solutions based on utilising PKI, digital signatures and certificates through a TA or Centralised Authority (CA) are widely discussed. With numerous solution and techniques, the aim of this study is to detect immediate research direction. Although there are several gaps in the domain of supply chain, big data, cloud security and so on, this research concentrates on liability and adaptive security. This is because present CAVs are resource-constrained to process large number of vehicular messages. Even if the messages are authenticated and executed there is no mechanism to account for the actions of the vehicle based on the message processed.

5.1. Liability

Automotive manufacturers during product procurement and assembly play a significant role. Errors and vulnerabilities in the supply and incorrect assembly could lead to catastrophic situations. One such example is Jeep Cherokee attack where the adversaries utilised compact cellular base station to access the Sprint network to instrument their attack on the vehicle. As a result, the vehicle, Jeep Cherokee, had the reputational damage even though the responsibility lied on the insecure Sprint network[6] . This highlights that a vulnerable commodity and third-parties could inflict damage on an automotive product and there exists limited research to address this issue of liability through security measures. Furthermore, the research on the methods to rectify a detected vulnerability is limited. This is due to the challenge of allocation and the conflict of business objectives.

Moreover, the security mechanism in third-party applications interacting with neighbouring vehicles are also under-researched further raising concerns on the ownership of data and the type of mutual authentication involved between different communicating entities that share information. This demands research on the privacy trade-offs with a third-party and evolving standardisation of secure collaboration and information exchange between external data processors and vehicles to ensure liability. For example, with authentication and validation, connected vehicles could also transmit malicious packets (Sybil attack or tampering with authenticated on-board vehicle equipment etc.). A situation such as these require immediate response to prioritise safety of the CAV after detection.

5.2. Adaptive Security

Cloud and edge-cloud technologies support CAVs with computation of a large amount of data [33, 38]. However, CAVs face challenges with long-life expectancy and deteriorating on-board computational capabilities in an evolving dynamic environment. At present, research in this domain is limited and there is a compelling need to ensure a secure, robust and efficient communication mechanism considering the ageing process between CAVs and cloud-assisted infrastructures. Therefore, there should be an to investigate the problem of providing reliable communication latency for V2X reliant safety-critical applications in CAVs.

The IEEE, ETSI and SAE standards have described ECDSA based cryptographic solutions for V2X communication. However, these solutions incur overheads and challenge computational capability and communication latency. Parameters such as encapsulation and decapsulation delay have been under researched on CAV platforms. Furthermore, different CAV models would have diverse ecosystems with distinct system architectures and data processing techniques, which would further introduce complexities and may distort the secure CAV's interoperability. Consequently, research to be conducted to address the issue of variability for introducing optimal security mechanisms for establishing an interoperable CAV ecosystem.

Studies on self-protecting software and adaptive systems are fast emerging. Yuan, et al.[11] discusses self-protecting software which inspires adaptive and opportunistic security. There are two broad categories: "Reactive" and "Proactive". Reactive software systems detect malicious data packets or repeated failures while the proactive software systems predict security threats, constraints and problems in advance to tune and mitigate them. Therefore, applying "Proactive" strategies with adaptive security techniques instead of static security mechanism for CAVS would be a suitable area to study the above-mentioned constraints.

Although "Proactive" strategies claim to prevent passive attacks; detection and mitigation mechanism for active attacks have been not addressed [39]. To do so, it requires a clear definition of the mechanism to perform systematic security scans, downgrades or upgrades which must be considered with developing security protocols. This capability supports adaptive security but may be help protect attacker's from performing low-cost downgrade attacks.

Nevertheless, there needs to be a vigorous way to determine the security deployed at any given instance to satisfy vehicular liability/accountability requirements. Subsequently, applying adaptive security with machine learning capabilities would help security state estimations and thereby predict what kind of security could be applied for a vehicular network bandwidth; however, research in this domain is at early stages.

6. Conclusion

Key security requirements are identified and discussed. Next, an analysis of threats is conducted by building a taxonomy. According to the threats, the challenges are addressed by discussing the countermeasures. Therefore, the four research objectives are duly answered by reviewing and gaining support from formulating the taxonomy. Furthermore, the research has contributed significantly to the major concerns for ensuring liability and emphasising the importance of adaptive security for evolving cloud-assisted CAV requirements. Selecting appropriate criteria for choosing security mechanism and achieving optimal security for overcoming the resource-constrained computation is a major research challenge. It has also raised concerns on the issues related to interoperability and liability when data can be processed across different entities.

7. Acknowledgment

This work is supported by the UK Hub for Cyber Security of the Internet of Things, PETRAS, under grant (EP/N02334X/1)

8. Reference

[1] C. Morris. (2017, 06/06). *Tesla Surpasses 4 Billion Miles of Vehicle Data - And Thats Just the Begining*. Available: https://evannex.com/blogs/news/tesla-surpasses-4-billion-miles-of-vehicle-data-and-that-s-just-the-beginning

[2] C. Urmson, "The self-driving car logs more miles on new wheels," *Google official blog,* 2012.

[3] S. O'Kane. (2017, 06/06). *Waymo's self-driving cars are racking up miles faster than ever*. Available: https://www.theverge.com/2017/5/10/15609844/waymo-google-self-driving-cars-3-million-miles

[4] A. Habeck *et al.*, "Connected car, automotive value chain unbound," McKinsey&Company2014.

[5] E. Hamida, H. Noura, and W. Znaidi, "Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures," *Electronics,* vol. 4, no. 3, pp. 380-423, 2015.

[6] C. Miller and V. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," *Black Hat USA, 2015.,* 2015.

[7] K. Koscher *et al.*, "Experimental Security Analysis of a Modern Automobile," presented at the 2010 IEEE Symposium on Security and Privacy, 2010.

[8] S. V. E. S. S. Committee, "SAE J3061-Cybersecurity Guidebook for Cyber-Physical Automotive Systems," *SAE-Society of Automotive Engineers,* 2016.

[9] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications,* vol. 1, no. 2, pp. 53-66, 2014.

[10] M. Zhao, "Advanced driver assistant system, threats, requirements, security solutions," *Intel Labs,* 2015.

[11] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," *Reliability Engineering & System Safety,* vol. 96, no. 1, pp. 11-25, 2011.

[12] M. Javed, B. Hamida, A. Al-Fuqaha, and B. Bhargawa, "Adaptive Security for Intelligent Tranport System Applications," 22 Sep 2017 2017.

[13] M. A. Javed, E. b. Hamida, and W. Znaidi, "Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice," *Sensors,* vol. 16, no. 6, Jun 15 2016.

[14] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A Survey of the Connected Vehicle Landscape--Architectures, Enabling Technologies, Applications, and Development Areas," *IEEE Transactions on Intelligent Transportation Systems,* vol. PP, no. 99, pp. 1-16, 2017.

[15] D. Shepardson. (2018). *Tesla says crashed vehicle had been on autopilot prior to accident*. Available: https://www.reuters.com/article/us-tesla-crash-idUSKBN1H7023

[16] J. Mullins, "Ring of steel II - New York City gets set to replicate London's high-security zone," *IEEE Spectrum,* vol. 43, no. 7, pp. 12-13, 2006.

[17] M. Müter, A. Groll, and F. C. Freiling, "A structured approach to anomaly detection for in-vehicle networks," in *Information Assurance and Security (IAS), 2010 Sixth International Conference on*, 2010, pp. 92-98: IEEE.

[18] A. M. Javed, S. Zeadally, and Z. Hamid, "Trust-based security adaptation mechanism for Vehicular Sensor Networks," *Computer Networks,* vol. 137, pp. 27-36, 2018.

[19] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks – A survey," *Computer Communications,* vol. 51, pp. 1-20, 2014.

[20] M. Yampolskiy, P. t. HorvÃ¡th, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "A language for describing attacks on cyber-physical systems," *International Journal of Critical Infrastructure Protection,* vol. 8, pp. 40-52, 2015.

[21] M. S. Al-Kahtani, "Survey on security attacks in Vehicular Ad hoc Networks (VANETs)," in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, 2012, pp. 1-9: IEEE.

[22] S. Checkoway *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," *In USENIX Security Symposium,* 2011.

[23] S. Kamkar, "Drive it like you hacked it: New attacks and tools to wirelessly steal cars," *Presentation at DEFCON, 23.,* 2015.

[24] M. Amoozadeh *et al.*, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine,* vol. 53, no. 6, pp. 126-132, 2015.

[25] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations," *Transportation Research Part A: Policy and Practice,* vol. 77, pp. 167-181, 2015.

[26] J. K. Gurney, "Sue my car not me: Products liability and accidents involving autonomous vehicles," *U. Ill. JL Tech. & Pol'y,* p. 247, 2013.

[27] C. Pinto, "How Autonomous Vehicle Policy in California and Nevada Addresses Technological and Non-Technological Liabilitie," *Intersect: The Stanford Journal of Science, Technology, and Society, 5,* 2012.

[28] R. H. Weber, "Accountability in the Internet of Things," *Computer Law & Security Review,* vol. 27, no. 2, pp. 133-138, 2011.

[29] S. Wahlbin, K. E. Rourke, and K. Wiesman, "Computerized method and system for estimating an effect on liability of the speed of vehicles in an accident and time and distance traveled by the vehicles," ed: Google Patents, 2010.

[30] E. Ben Hamida and M. A. Javed, "Channel-Aware ECDSA Signature Verification of Basic Safety Messages with K-Means Clustering in VANETs," presented at the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016.

[31] J. P. Hubaux, S. Capkun, and L. Jun, "The security and privacy of smart vehicles," *IEEE Security & Privacy,* vol. 2, no. 3, pp. 49-55, 2004.

[32] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: Identity and credential management in vehicular communication systems," *IEEE Vehicular Technology Magazine,* vol. 10, no. 4, pp. 63-69, 2015.

[33] M. H. Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," *IEEE Vehicular Technology Magazine,* vol. 12, no. 2, pp. 45-51, 2017.

[34] ABI. (2018, 16/4). *Connected Vehicle Cloud Platforms*. Available: https://www.abiresearch.com/market-research/product/1022093-connected-vehicle-cloud-platforms/

[35] S. Senior, C. Rec, H. Nishar, and T. Horton, "AWS Connected Vehicle Solution," Amazon2018.

[36] Z. Fu, W. Hu, and T. Tan, "Similarity based vehicle trajectory clustering and anomaly detection," in *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, 2005, vol. 2, pp. II-602: IEEE.

[37] U.S Department of Transportation. (2016). *Cybersecurity best practices for modern vehicles*.

[38] L. Bariah, D. Shehada, E. Salahat, and C. Y. Yeun, "Recent Advances in VANET Security: A Survey," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, 2015, pp. 1-7.

[39] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems,* vol. 14, no. 1, pp. 284-294, 2013.

Cause		**Effect**		**Action**		**Counter- measures**	**Proximity of the attack**	**Scalability of the attack**
Influenced element	**Influence**	**Affected Element**	**Impact**	**Method**	**Preconditions**			
What is the object of manipulation?	**What is changed on the influence element?**	**What object has been influenced the manipulation?**	**What has been changed because of the attack?**	**How the influence is performed?**	**What are the prerequisites for executions of the methods?**			
Basic safety messages	Speed data	Overall Vehicle Speed	Increase in Traffic in the targeted and nearby roads	Malicious advertisers (V2V/V2I) generate congestion responses based on congestion requests	- Parked Bot Cars that are infected - Compromised Cars	Correlation of messages from neighbouring vehicles and cross verification	Remote Access	High
Telematics ECU's Unix-like operating system	Access to program handling Bluetooth functionality	Bluetooth Connectivity	Execution of any arbitrary code and taking control of the entire Vehicular systems	**Indirect and Direct Bluetooth access:** Vulnerability present in the interface code of the Bluetooth enabled telematics system. Requires pairing of adversarial device to Bluetooth	Attacker needs to pair with the vehicles on-board system	Restrict access	Remote Access	Small and Large
Uconnect and Vehicle's On-board telematics systems	Vehicles on-board connectivity feature and CAN bus vulnerabilities - Jeep Cherokee Uconnect and Sprint's network	* Vehicles brakes * Engine * Horn * Transmission	* Adjust AC temperatures * Adjusting radio volume * Windshield with wiper fluid * Disable transmission * Control the throttle * Disable the brakes	Remote access to vehicles communication system with the ability to flash the firmware version	Availability of Uconnect's D-Bus Port to be open and able to communicate with the open D-Bus Port.	* Code Robustness * Restricted access to OD and Patching software's	Remote Access	High
Relay of Low Frequency and Ultra High Frequency signals through generation of magnetic fields to trigger the Passive keyless entry system's (key fob) antenna	Relay over the Cable Attack - Relay over the cable using antennas in order to send open and start message over the UHF channel	Passive Keyless Entry systems, Vehicle unlocking and Ignition system	*Unlocking the vehicle doors. * Starting the vehicle	Usage of two antennas with an amplifier. One placed near the door handle to capture the beacon which is transmitted to the other end creating current and magnetic inducing the PKES which would demodulate and message from the car.	A set up of two antennas with cable with close proximity to the vehicle.	* Shielding the Key * Removing the Battery from the Key * Software only modification * Access Control restriction * Hardware Modification	Remote Access	High
Vision sensors (Camera)	Not able to tune the auto exposure -	*Environmental Light considering the light wavelength and distance between the camera	Incorrect model recognition	Bright (250 lx) and dark (0 lx) environments, with different light sources at multiple distances (50 cm, 100 cm, 150 cm and 200cm)	Close proximity to vehicular camera	*Introduction of multiple cameras for redundancy checks	Physical	High
Range Sensors (radar, Ultrasonic, LiDar)	* Relay of signal * Spoofing of signal	* Light Transceivers/Pulse Generator	Incorrect data sensed which could cause trivial vehicular impacts	When the attacker receives the Lidar signal and relays then to next vehicle	Working knowledge of Lidar and set of transceivers	*Introducing Redundant Lidar sensors * Random probing * Probing multiple Times * Shortening pulse period	Remote Access	High

Table 4: Attack taxonomy and countermeasures