Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments

Benyahya, Meriem; Collen, Anastasija; Kechagia, Sotiria; Nijdam, Niels Alexander

How to cite

BENYAHYA, Meriem et al. Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. In: Computers & security, 2022, vol. 122, p. 102904. doi: 10.1016/j.cose.2022.102904

This publication URL: https://archive-ouverte.unige.ch/unige:164571
Publication DOI: 10.1016/j.cose.2022.102904

Computers & Security 122 (2022) 102904

Contents lists available at ScienceDirect

Computers & Security

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

Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments

Meriem Benyahya[a,*], Anastasija Collen[a], Sotiria Kechagia[b], Niels Alexander Nijdam[a]

[a] Centre Universitaire d'Informatique, Geneva School of Economics and Management, University of Geneva, Geneva, Switzerland
[b] Faculty of Law, University of Geneva, Geneva, Switzerland

ARTICLE INFO

Article history:
Received 29 July 2021
Revised 7 February 2022
Accepted 28 August 2022
Available online 2 September 2022

Keywords:
Automated city shuttles
Connected automated vehicles
Shared mobility
Cybersecurity
Data privacy

ABSTRACT

The Automated City Shuttles (ACSs) aim to shape the future public transportation and provide more efficient and accessible mobility in smart cities. With the absence of a driver, such mini-busses process the sensors' inputs and exchanged data with other vehicles and intelligent transport systems to achieve a real time assimilation of its surroundings. Consequently, the technologies supporting the driverless functionalities ushered new cybersecurity risks and data privacy breaches. Unfortunately, several studies mostly focus on individual Connected-Automated Vehicles (CAV), though intrinsic underpinnings of the ACS's threat vectors remain unexplored. In the present paper, we considerably extend that investigation by proposing a comprehensive state of the art with farsighted analyses addressing security threats and data privacy concerns from both technical and legal perspectives to thwart potential attacks. Moreover, as existing approaches have not provided yet a clear road map about ACS's security standards, the present work sheds light on recent and up to date standards and standardisation bodies dealing with cybersecurity and privacy issues in the automated driving ecosystem. This paper presents an analysis debating the trade-off between maximising the ACS benefits and minimising the associated security vulnerabilities and attacks through an overview of technical and legal mitigation strategies.

1. Introduction

Within the last few years, cities have been acquiring management approaches based on new technologies to enhance citizen's quality of life. Modern cities are motivated to provide new shared mobility services with higher efficiency and reliability at lowest costs. Integrating ACSs to the urban environment is one effective manner to tackle this challenge. ACSs introduce an innovative public transportation paradigm through customised offers like on-demand and door-to-door services (Iclodean et al., 2020). Meyer et al. (2017) demonstrated how the automated vehicles can improve the public transportation in Swiss municipalities by increasing its accessibility up to 40%. As ACSs are providing a non stop service, they are expected to reduce drivers payroll costs to public transportation companies (Lin et al., 2019) and provide cheaper commuting for the passengers (Bösch et al., 2018). In addition, integrating such mini-buses, with extensive automated capabilities, to the public transportation promises more accessibility to elderly, children and disabled users (Collingwood, 2017; Daniel J. Fagnant and Kockelman, 2015). ACSs can also decrease accidents per the absence of the human factor error, improve traffic flow and road transport capacity (Lim and Taeihagh, 2018). Based on such assumptions, ACSs will not just improve the passengers' experience, but they will beneficially change the urban dimensions and push it forward to a new era.

Driverless vehicle can be a personal individual car, a taxi, a bus, a shuttle or a mini-bus, an emergency car, a truck, a train, a tram, etc. with different levels of human involvement (Boukerche et al., 2017). The Society of Automotive Engineering (SAE) defined a complete range of six automation levels varying from level 0, where none of the safety-critical functions are automated, to level 5, presenting a full automation of control systems (SAE, 2018). In addition, the regulation 2019/2144 of the European Parliament and of the Council of 27 November 2019 defined "Fully Automated Vehicle" to be motor vehicle operating autonomously without the human supervision and intervention (The European Parliament and of the Council, 2019). The present paper concentrates on ACS as fully automated mini-buses for public transportation with levels 4 and 5 from the SAE classification.

* Corresponding author.
E-mail addresses: meriem.benyahya@unige.ch (M. Benyahya), anastasija.collen@unige.ch (A. Collen), sotiria.kechagia@unige.ch (S. Kechagia), niels.nijdam@unige.ch (N.A. Nijdam).

https://doi.org/10.1016/j.cose.2022.102904

ACS represents a unique challenge not only by deploying the latest Information Communication Technologies (ICT) advancement into the public transportation sector, but also by expanding the existing city's infrastructure into smart enabled environment. This process involves several upgrades and adaptation, including the city infrastructure, the social and economic impacts, political aspects, cybersecurity challenges, implementation of relevant regulations and standardisation which should come to support the ACS deployment. In this paper, we focus on cybersecurity threats, data privacy issues and their related regulations and standards as critical challenges that can be very harmful to ACSs' integration if not well considered. The concern remains about the trade of maximising the ACS benefits and minimising associated vulnerabilities and attacks' unintended outcomes.

Collard et al. (2017) have updated the cybersecurity definition based on the last years challenges related to Internet of Things (IoT). The authors defined cybersecurity as the organisation and the protection of information technologies with the combination of the following notions: availability, confidentiality, criticality, attack impact, integrity, ownership, sensitive values, legal risk, contextualisation, risk assessment and information storage (Collard et al., 2017). Applied to Internet of Vehicles (IoV) paradigm, National Highway Traffic Safety Administration (NHTSA) defined cybersecurity as the protection of the vehicle components, infrastructure and communications from any harmful attacks, unauthorised access or anything that jeopardises the safety functions (NHTSA, 2021). Given that the ACS functioning depends on many in-vehicle hardware and software systems in addition to a permanent connection to the external environment, the risk of vulnerabilities escalates.

The existing literature has witnessed multitude of successful attacks in the last decade over automated driving components. Miller and Valasek (Miller and Valasek, 2015) presented how they remotely attacked the Controller Area network (CAN) bus of the Jeep Cherokee causing a loss of control over the braking and the steering systems. Zhang et al. (2014) described the operational and safety disruptions that may be caused by a malware if it infects the connected vehicles' Electronic Control Units (ECUs). Yan et al. (2016) demonstrated how automated driving sensors in Tesla S can be blinded and led to a crash. With the increase of interest in deploying automated driving within public transportation, the motivation and the likelihood to conduct similar attacks will grow. This is why we consider of great interest to analyse, based on security-by-design mechanisms, the potential cybersecurity threat vectors and their technical and legal countermeasures in the present paper.

As the ACS moves from one place to another, it communicates permanently with other vehicles, infrastructure and external devices. While moving, the shuttle exchanges data also with its passengers. The shuttle's user may be requesting customised ACS services which requires the integration of location-based services (LBS), such as Mobility as a Service (MaaS). MaaS is a mobility platform which bridges public transport to mobility services by providing, for example, door-to-door services based on the passengers information including their location (Smith and Smith, 2020). Such new transport model requires an endless exchange of information, among vehicles, public transportation interfaces, users' smart devices and other third parties, which raises data privacy concerns (Murati and Hënkoja, 2019).

In the scientific literature, there are several definitions of data privacy. These definitions vary depending on the sector that explores them and prove that data privacy is a notion with many facets (Lin and Kifer, 2014). With the growth of IoT technologies, data privacy is perceived as the protection from any unauthorised access and usage control of the collected, processed and stored individuals information (Karnouskos and Kerschbaum, 2018). Applied to the IoV context, it refers to the vehicle passengers' privacy and the vehicle location (Manivannan et al., 2020). In other words, while exchanging messages with other vehicles and external devices, the ACS and the passengers' identities and locations should not be revealed (except to relevant authorities). Unlike the individual CAV, where such risk impacts a limited number of people, in the ACS the data privacy concern is applicable to a larger group of individuals, including the shuttle operators and passengers. Hence, considering the increased scope of the impact, in comparison to CAVs, data privacy in ACS must be looked at differently by incorporating adapted countermeasures and referring to existing laws, policies and standards.

In a context of exploring cybersecurity and data privacy threats, there has been much work conducted on studying attacks and countermeasures over CAVs (Dibaei et al., 2020; El-Rewini et al., 2020; Khan et al., 2020; Kim et al., 2021; Parkinson et al., 2017; Petit and Shladover, 2015; Petit et al., 2015; Ren et al., 2020; Suo et al., 2020). Though, the existing work didn't cover all potential threats and mitigation solutions comprehensively. It has also discussed the threats in a generic way without addressing the specificity of ACSs. In addition, data privacy concerns were extensively analysed in the literature but either as one of the threats (Cui et al., 2019; Pan et al., 2017; Sarker et al., 2020) or from liability perspective (Crane et al., 2017; Krontiris et al., 2020; Pattinson et al., 2020; Taeihagh and Lim, 2018; Veitas and Delaere, 2018) without a thorough review or a designation of applicable protocols, preserving privacy, while exchanging personal data within the vehicular environment. Organisational solutions to prevent from personal data breaches within automated vehicles as a means of public transport are also barely over-viewed. Furthermore, regulations and standards, related to cybersecurity and data privacy, were partially discussed (Al Mamun et al., 2018; Ali and Li, 2020; Lim and Taeihagh, 2018; Lonc and Cincilla, 2016; Lu et al., 2019; Schmittner et al., 2020; Schmittner and Macher, 2019; Schoitsch and Schmittner, 2020), sometimes with a focus on a single regulation (Costantini et al., 2020) or an individual standard (Macher et al., 2020; Schmittner et al., 2016) or just as an open issue for future research efforts (Cui et al., 2019). To the best of our knowledge, the existing research proposals neither provide comprehensive technological and legal guidelines for the ACS deployment nor identify the key standards for such vehicles' security certifications. A detailed description of other researchers' efforts along with a comparison between our efforts and their findings are highlighted in Section 2.

This trend encourages for a new breed of in-depth analysis and exhaustive statement of the state of the art, combining and focusing on three areas: cybersecurity, data privacy and related regulations and standards over ACSs. Our added value and main contributions are summarised as follow:

- A comprehensive review and a classification of surface attacks and how they are exposed to potential threats per the heterogeneous nature of ACSs.
- A mapping between the attacks and their corresponding mitigation strategies by recommending a combination of countermeasures per attack type based on an overview of the advantages and disadvantages of each mitigation scheme.
- Advocate a set of security and privacy regulations and guidelines that the stakeholders should bear on to have a valid approach on protecting the ACSs system.
- Elevate the existing privacy preserving schemes further by discussing their strengths and weaknesses and how they are applicable to the exchanged data within the ACS ecosystem.
- Based on a thorough investigation of road vehicle, safety, vehicular cybersecurity, data privacy, public transport, Intelligence Transport System (ITS) and IoT related standards; a selection of up to date standards is provided to point out not only the pub-

lished but also the under development ones that are promising security and privacy by design deployment for the ACS.

This article addresses the following questions:

- RQ1: What are the existing cybersecurity and data privacy risks related to ACSs? Can a specific mapping between the threat vectors and the countermeasures help in accurately shielding the ACS' environment?
- RQ2: Would individuals' privacy remain preserved while using ACSs? Would the implementation of powerful privacy preserving protocols be enough to protect personal data processed within the ACS's system?
- RQ3: What are the technical and legal strategies to mitigate or reduce the identified risks? And what are their limitations?
- RQ4: Is there an existing framework or standards addressing the security compliance relevant only to ACSs?

The remainder of this paper is structured as follows: Section 2 discusses the related work and a comparison of the present work with those previously published. Section 3 presents an overview of classified cybersecurity threats. This section identifies two layers impacting security of the ACS: the in-vehicle equipment and external communications. It also presents the existing risk mitigation plans and the regulations covering such security threats. Section 4 gives an overview of data protection risks, the existing technical solutions to offset such threats and the regulatory frameworks aiming to preserve privacy within the ACS ecosystem. Section 5 describes existing standards and those under development supporting the shuttle resiliency, including the protection from data privacy leakage. Section 6 acknowledges the present research limitations and provides a discussion over the future work orientation. Finally, Section 7 offers concluding remarks on the state of the art.

2. Related work

In recent years, few papers focused their interest on ACSs as a means of public transportation. Iclodean et al. (2020) evaluated the safety and social implications related to the technological solutions implemented within ACSs. Ainsalu et al. (2018) studied ACSs' energy efficiency and their legal framework with regard to civil liability. Although, research works did not address cybersecurity and data privacy concerns over ACSs.

Motivated by the safety risk of cybersecurity attacks in the vehicular environment, multiple literature reviews discussed security threats and data privacy concerns. Petit and Shladover (2015) highlighted the consequences of remote or direct access attacks over CAVs. Parkinson et al. (2017) addressed the challenges and knowledge gaps facing the IoV sector from cybersecurity vulnerabilities perspective. Cui et al. (2019) presented the inter-relation between CAVs safety failures and security attacks; in addition to a broad mapping of potential attacks impacting the data privacy and their eventual countermeasures. Ren et al. (2020) drew in depth threats related to sensors and in-vehicle communication networks. The authors stated security guidelines including recommendations for privacy preservation. Dibaei et al. (2020) investigated attacks and defences to shield the automated environment while presenting detailed technical mitigation strategies.

Recent researchers have drawn more comprehensive frameworks, such as Khan et al. (2020) and El-Rewini et al. (2020), discussing potential attacks and their respective mitigation strategies with a particular focus on communication challenges. Kim et al. (2021) presented a new classification of attacks and defences over CAVs. Suo et al. (2020) presented cybersecurity threats through a fault tree view. They also classified the existing mitigation solutions through a layered view with a focus on location-based schemes to countermeasure the location leakages while communicating with the infrastructure.

The majority of the cited works have introduced few standards at glance or as an expected effort for the future work without a profound review of the standards' implication within the driverless vehicles' environment. Very few papers (Costantini et al., 2020; Lonc and Cincilla, 2016) presented International Organization for Standardization (ISO) and European Telecommunication Standards Institute (ETSI) as unique existing standardisation bodies related to the automated driving environment. The most detailed reviews were published by Schmittner, in collaboration with other authors (Macher et al., 2020; Schmittner et al., 2020; 2016; Schmittner and Macher, 2019; Schoitsch and Schmittner, 2020). Though, the efforts remain limited to the automotive cybersecurity risk management tools without an exhaustive identification of all existing regulations and standards.

Per the analysis from Table 1, we differentiate from the aforementioned works by:

- Focusing on the ACS as a special case of CAVs ecosystem.
- Presenting an in-depth analysis on attacks and mitigation strategies.
- Presenting an interdisciplinary and comprehensive approach regarding cybersecurity and data protection by connecting the technological cyber defences with the existing regulatory and policy privacy frameworks as well as the security standards.

3. Cybersecurity threats

To ensure safety and security of the ACS, it is crucial to depict the system attack surfaces and build the required shields accordingly. Academic researchers have been debating the different types of attackers, attacks, and attack surfaces to identify adequate mitigation plans.

Attackers can be internal or external, malicious or rational, active or passive and intentional or unintentional as described by Cui et al. (2019). The internal active attacker deploys an attack on purpose with an authenticated profile by sending malicious packets in the network (for example) while the external passive attacker is an intruder who is eavesdropping the system. On the other hand, a rational attacker seeks personal profit while an unintentional attacks occur by coincidence or due to an equipment failure.

Based on the attacker profile and type, similar works discuss two groups of CAVs related attacks. Petit and Shladover (2015) presented the "Autonomous Automated" surface attacks, defined as all in-vehicle surfaces through which an attack can be accomplished; and "Cooperative Automated" referring to infrastructure and communication surfaces which can be targeted by an attacker. Van Wyk et al. (2020) classified the attack surfaces as internal (referring to in-vehicle devices, vehicle sensors, and in-vehicle networks) and external (like communication interference with other vehicles and devices). As a result, our work was built on the categorisation of two cybersecurity layers as potential attacks entry points impacting the ACS ecosystem:

- *In-vehicle threats*: defining any in-vehicle component through which an attack can be conducted. It covers the potential vulnerabilities on the vehicle sensors, the ECUs data flows and in-vehicle communication networks as described in Fig. 1.
- *Communication threats*: refer to the communication with, public transportation and city infrastructure (Vehicle-to-Infrastructure (V2I)), other vehicles (Vehicle-to-Vehicle (V2V)), and any surrounded devices or services (Vehicle-to-everything (V2X)) as shown in Fig. 2.

Table 1
Related work comparison.

Related work	Year	Scope		Cybersecurity				Data privacy			Standards		
		ACS	CAV	In-V. attacks	Ext. attacks	Mitigation	Regulations	Risk	Mitigation	Regulations	ISO	ETSI	Others
Iclodean et al. (2020)	2020	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗
Ainsalu et al. (2018)	2018	✓	✗	✗	✗	✗	✓	✗	✗	✓	✓	✗	✗
Petit and Shladover (2015)	2015	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗
Parkinson et al. (2017)	2017	✗	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗
Cui et al. (2019)	2019	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
Ren et al. (2020)	2020	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗
Dibaei et al. (2020)	2020	✗	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	✗
Khan et al. (2020)	2020	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗
El-Rewini et al. (2020)	2020	✗	✓	✗	✓	✓	✗	✓	✓	✗	✗	✗	✗
Kim et al. (2021)	2021	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✗
Suo et al. (2020)	2020	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗
Lonc and Cincilla (2016)	2016	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗
Costantini et al. (2020)	2020	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓
Schmittner and Macher (2019)	2019	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✓
This work		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

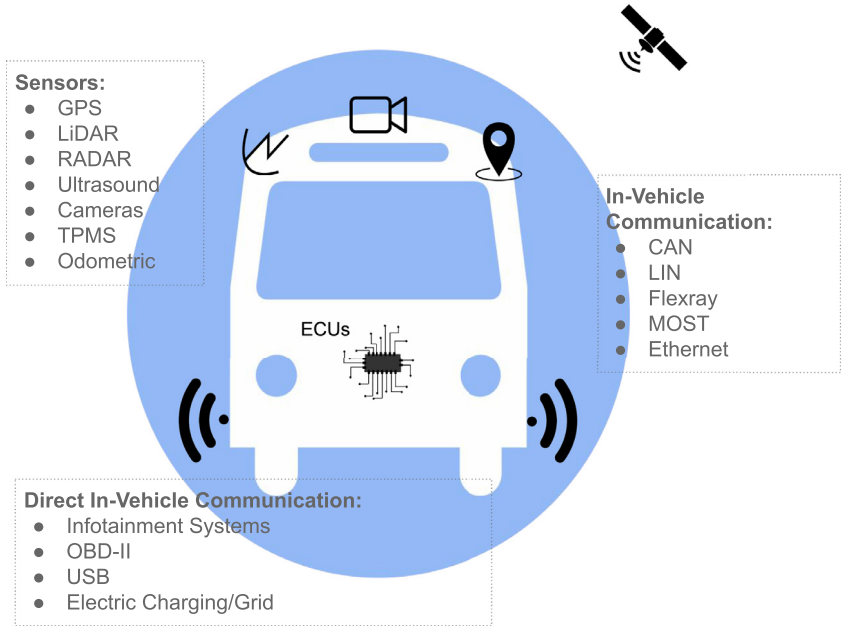

Fig. 1. In-vehicle surface attacks.

3.1. In-vehicle threats

3.1.1. In-vehicle sensors

With the absence of the human driving in the ACS, the passenger's safety depends completely on the vehicles' sensors and their interpretations to the collected inputs. Based on such information, the ACS builds a picture of its surroundings to drive in the correct path, detects obstacles in a real time manner and, hence, avoid collisions (Wang et al., 2019). Sensors are expected to have numerous advantages to the automated driving (Petit et al., 2015). However, they can be victims to potential security breaches. Considerable collections of research identified attacks targeting the in-vehicle sensor systems (Parkinson et al., 2017; Ren et al., 2020; Sarker et al., 2020; Wang et al., 2019; Yan et al., 2016). This subsection presents the most discussed in-vehicle sensors vulnerabilities and the most known attacks on them as summarised in Table 2.

Differential Global Positioning Systems (GPS), which is a widely used Global Navigation Satellite System (GNSS), provides positioning, navigation and time services to ACSs (Elliott et al., 2019). Accurate GPS positioning data is one of the critical inputs enabling safe self-driving, yet such technology has been potentially concerned with cyber-attacks (Li et al., 2020). Spoofing and jamming are the most common GPS attacks leading to disrupt sensor readings. A spoofing attack happens when an incorrect but valid GPS signals are sent to mislead the positioning (Zeng et al., 2018). In the recent simulation of Dasgupta et al. (2021), a sophisticated spoofing attack was conducted by mimicking GPS signal and broadcasting falsified location coordinates. On the other hand, a jamming attack occurs when noise is transmitted on the GPS frequency preventing the GPS from distinguishing the accurate signals (Parkinson et al., 2017).

Light Detection and Ranging (LiDAR) is a key sensor to automated driving in any light condition. The sensor provides functionalities such as behaviour predictions, collision avoidance, pedestrian detection and object recognition (Changalvala and Malik, 2019). LiDAR offers a 360° view and 3D perception by fir-

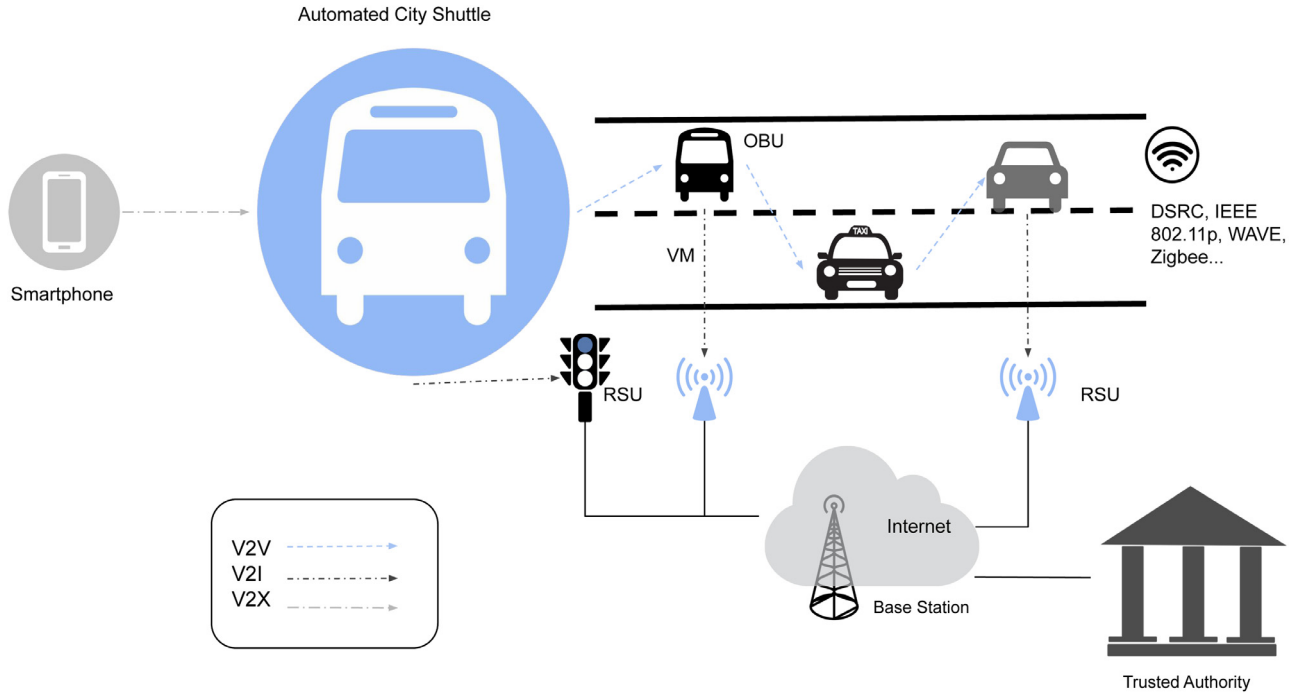

Fig. 2. ACS communication modes.

Table 2
Sensors threats summary.

Sensor	Signal type/inputs	Automated driving function	Type of attacks	Demonstration reference
GPS	Microwave	Navigation	Spoofing Jamming	Dasgupta et al. (2021); Zeng et al. (2018)
LiDAR	Laser Pulses	Behaviour prediction Collision avoidance Pedestrian detection Object recognition	Spoofing Jamming Relay Tampering	Cao et al. (2019); Changalvala and Malik (2019) (Petit et al., 2015)
RADAR	Radio Waves	Collision avoidance Object recognition	Spoofing and Jamming	Sarker et al. (2020); Yan et al. (2016)
Acoustic / Ultrasonic	Ultrasound Waves	Parking and Backing	Spoofing Jamming Quieting	Xu et al. (2018); Yan et al. (2016)
Cameras	Visible Light	Pedestrian detection Object recognition Lane detection Traffic sign detection	Blinding and Fooling	Petit et al. (2015); Yan et al. (2016)
TPMS	Tire Measurements	System decision	Falsifying Tampering	Daimi and Saed (2018)
Odometric	Data Fusion	Navigation Orientation	Fooling	Toledo et al. (2018)

ing laser pulses, getting back their reflections and hence perceive a point cloud used for object detection (Cao et al., 2019). Several researchers recorded LiDAR's vulnerability to spoofing, jamming, relay and tampering attacks leading the vehicle to assume nonexistent obstacles and to a halt. Cao et al. (2019) demonstrated a successful spoofing attack by replaying laser pulses from a malicious device at the roadside and hence creating an erroneous point cloud. Petit et al. (2015) conducted remotely a successful relay attack by making objects appear either closer or further than they really are. In addition, LiDARs are vulnerable to data tampering attacks that can be launched from inside the vehicle (Changalvala and Malik, 2019). Such attacks happen when a hacker gets access to the in-vehicle network interfaces like CAN and execute by modifying/tampering the LiDAR's point cloud. Changalvala and Malik (2019) identified two types of data tampering attacks: Fake Object Insertion (FOI) and Target Object Insertion (TOD). As a matter of fact, when data is tampered either by inserting fake data (FOI) or by removing existing one (TOD), decision making units will be impacted leading the vehicle to a prompt halt (Parkinson et al., 2017; Yan et al., 2016).

Similar to LiDAR, but using radio waves instead of laser signals, **Radio Detection and Ranging (RADAR)** provides the object recognition and collision avoidance functions to driverless vehicles (Sarker et al., 2020). ACSs use two main radar types: Short Range Radar (SRR) to detect objects at short - called also Millimetre Wave Radar (MMW)- and Long Range Radar (LRR) for long distances (up to 150 m) (Yan et al., 2016). Additionally, RADARs support the automated driving by detecting the speed and direction of other objects heading toward it (Sarker et al., 2020). However, by using the same frequency band, the signal can be spoofed or jammed causing the vehicle to be fooled, to presume nonexistent obstacles or to fail in detecting objects as demonstrated by Yan et al. (2016).

Acoustic sensors, called also ultrasonic sensors, work similarly to LiDAR and RADAR, but using ultrasound waves (called pings) instead of light or radio signals (Xu et al., 2018). Such sensors are mainly used for backing up or parking purposes by sending high frequency sound waves to measure echoes to determine the distance to objects (Sarker et al., 2020). Researchers have demonstrated how acoustic sensors can be victims to quieting attacks, where noise and/or echoes can be eliminated, preventing the vehicle from receiving the echoes required to measure distance to objects (Yan et al., 2016). Acoustic sensors can be spoofed or jammed causing the vehicle to hit unperceived surroundings, as demonstrated in Tesla S by Xu et al. (2018).

In addition to GPS, LiDAR, RADAR, ultrasonic, and other sensors, **cameras** are required to insure safe automated driving, though, they can be blinded or fooled too. Yan et al. (2016) demonstrated how cameras can be blinded or permanently damaged with malicious optical inputs (laser and LED) using low cost resources. The authors named the demonstration "blinding attack" causing undesired vehicle breaking or deviation from planned trajectory or road navigation. When blinded, important functions to the automated driving are disrupted such as lane detection, traffic sign recognition, pedestrians or any other physical obstructions (Parkinson et al., 2017). Petit et al. were also successful to blind the vehicle cameras using a simple laser pointer, disabling the vehicle from detecting the vehicle ahead (Petit et al., 2015).

Tyre Pressure Monitor Systems (TPMS) is another vulnerable small sensor which is essential in all vehicles, including non automated ones (Parkinson et al., 2017). The TPMS broadcasts non-encrypted tire measurements like air pressure and temperature to the TPMS ECU (Daimi and Saed, 2018). Since the transmitted data is not encrypted, the sensor can be easily attacked as the message can be replaced by a false one or modified to hide important tyre information.

Odometric systems include wheel encoders and gyroscope sensors which are used for inertial-odometric navigation (Petit and Shladover, 2015). Such equipment aims to compute the vehicle position and movement by fusing data from the wheel readings (rotation and velocity) and the vehicle sensors (GPS, RADAR) to predict changes in position (Toledo et al., 2018). Obviously, if falsified data is computed, the vehicle orientation is impacted, leading to a wrong system decision making.

3.1.2. In-vehicle communication

The in-vehicle communication occurs by transmitting messages between the vehicle ECUs, the vehicle ports and the infotainment systems (El-Rewini et al., 2020). Such messages' transmission is enabled by the vehicle bus systems. This section highlights the threats related to the vehicle internal communication system.

The discussed attacks in Section 3.1.1 might impact implicitly or explicitly the vehicle **ECUs** which are vulnerable to direct attacks too. ECUs are the most important in-vehicle component as they are controlling the vehicles' system and subsystems by receiving and processing broadcast signals from the sensors (Pan et al., 2017). Compared to non automated vehicles, the number of ECUs has been incremented in ACSs as they are responsible for the automated driving decisions (Klinedinst and King, 2016). With the increased number of ECUs, the lines of codes are expended too, enlarging the risk to code vulnerabilities (Parkinson et al., 2017).

ECUs communication occurs by exchanging network packets through heterogeneous in-vehicle communication protocols such as CAN, Local Interconnect Network (LIN), Media-Oriented System Transport (MOST), FlexRay and Ethernet (Daimi and Saed, 2018; Pan et al., 2017). Each protocol supports different communication within the vehicular network; however, they embed multiple security concerns. Researchers showcased multiple attacks such as Denial of Service (DOS) (El-Rewini et al., 2020), packet injection (Miller and Valasek, 2015), sniffing / eavesdropping (Dibaei et al., 2020), spoofing (Yan et al., 2016), relaying, and bus-off (Cho and Shin, 2016) over the in-vehicle communication networks.

CAN buses are famous for their low cost, high bandwidth and flexibility; though, they were not designed with high security concerns (Wu et al., 2020). First, the packets can be easily sniffed or falsified since they are broadcast into all nodes without containing any authentication information (Changalvala and Malik, 2019). Second, the malicious packets can't be back-traced as the packets are not associated with a CAN ID (Pan et al., 2017). The Keen Lab identified 14 vulnerabilities and demonstrated an attack over the BMW X5 where the vehicle was completely controlled by getting access to its CAN bus (Zorz, 2018). Upgrades have been rolled out by the car manufacturer; though, with the increase of wireless communications on ACSs, further attacks might be witnessed if CAN's vulnerabilities are not adequately addressed.

LIN may substitute the CAN for transmissions where high bandwidth is not required (El-Rewini et al., 2020). It is a cheaper communication protocol that is mainly used for the vehicle control (like seats and doors) and which communicates in a master-slave mode (Ernst and Michaels, 2018). Hence, if the master node is compromised, false data is then sent to all the LIN slave nodes as demonstrated through a rogue attack by Ernst and Michaels (2018). Takahashi et al. demonstrated that the response collision and header collision attacks are occurring when messages are not synchronised between master and slave nodes leading to undesired vehicle controls like keeping doors open (Takahashi et al., 2017).

The security of CAN and LIN buses has been rigorously studied, however the other in-vehicle networks are subject to malicious intentions too. **Flexray** is designed to be the next generation of the in-vehicle communication protocol with its high reliability and data rates; though, like CAN, it lacks confidentiality and authentication implementation (Ren et al., 2020). Flexray transmission has static and dynamic segments which are vulnerable to spoofing, eavesdropping, injection and replay attacks (Dibaei et al., 2020; El-Rewini et al., 2020; Ren et al., 2020). Additionally, **MOST** is mainly designed for media transfer with its high data rate that is considered 10 times faster than the Flexray and 100 times higher than the CAN (Ernst and Michaels, 2018). The communication in the MOST is synchronised by time frames which makes it vulnerable to jamming or DOS attacks if the synchronisation is disrupted (El-Rewini et al., 2020). Last but not least, **Ethernet** is another promising protocol providing cost and bandwidth advantages (Wu et al., 2020). Like in normal computer networking, Ethernet consists of hosts and switches which may add more vulnerabilities to the vehicle if attackers access to an open port on a switch. Hence, once access is gained, any further attack can take place like DOS, sniffing or falsifying impacting the confidentiality and integrity of the vehicle (El-Rewini et al., 2020).

Additional **physical ports** can present the point of entrance of an attack over the in-vehicle network. On-board Diagnostics System (OBD-II) port is designed mainly for the vehicle monitoring and system upgrading. However, if accessed by a malicious actor, all the vehicle data can be gathered and any of the listed attacks in Table 3 may occur (Khan et al., 2020). Moreover, USB ports present additional risks in modern vehicles, generally, and ACS, specifically, as attacks can inject malware and viruses into the system leading to endless attacks scenarios (Maple et al., 2019). Furthermore, the electric charging port has been studied as an additional surface attack. Bhusal et al. (2020) highlighted the risks of Man in the Middle (MitM), DOS, and false data or malware injection

Table 3
High level summary of attacks and their corresponding mitigation techniques.

Attack	Surface attack	Mitigation	References
Spoofing	GPS LiDAR RADAR Acoustic sensors In-vehicle networks	Redundancy Randomisation Cryptography BC MDL	(Li et al., 2020) (Bailey, 2018) (Shin et al., 2017) (Sheehan et al., 2019) (Bezemskij et al., 2018)
Jamming	GPS LiDAR RADAR Acoustic sensors In-vehicle network V2V	Redundancy Cryptography Firewalling BC	(Petit and Shladover, 2015) (El-Rewini et al., 2020) (Pesé et al., 2017)
Relay/ Replay/ MitM	LiDAR Vehicle Ports In-vehicle network V2V V2X	Redundancy Cryptography Firewalling BC	(Dibaei et al., 2020) (Pesé et al., 2017) (Khanam et al., 2020)
Tampering/ Falsifying	LiDAR TPMS Odometric sensors V2I	Redundancy Cryptography	(Daimi and Saed, 2018)
Quieting	Acoustic sensors	Redundancy Fusion	(Yan et al., 2016) (Xu et al., 2018)
Blinding	Cameras	Redundancy	(Parkinson et al., 2017) (Petit et al., 2015)
DOS	In-vehicle networks Vehicle ports V2I	Redundancy Cryptography Firewalling BC IDS	(El-Rewini et al., 2020) (Wu et al., 2020) (Ali Alheeti and Mc Donald-Maier, 2018) (Pesé et al., 2017)
Sniffing	In-vehicle networks V2X	Cryptography BC IDS	(Oham et al., 2021)
Malware Injection	In-vehicle networks Vehicle ports V2X	Cryptography IDS	(Zhang et al., 2014) (Maple et al., 2019)
Rogue	In-vehicle networks	Cryptography IDS	(Ernst and Michaels, 2018)
Bus-off	In-vehicle networks	Cryptography IDS MDL	(Kang and Kang, 2016)
Eavesdropping	In-vehicle networks V2I	Cryptography IDS	(Ren et al., 2020) (Khanam et al., 2020)
Bogus Information	V2V	Cryptography	(El-Rewini et al., 2020)
Sybil	V2V	Cryptography	(Dibaei et al., 2020) (El-Rewini et al., 2020)
Timing	V2V	Cryptography Firewalling	(Dibaei et al., 2020) (Bhargava et al., 2016) (Khanam et al., 2020)
Impersonation	V2I V2X	Cryptography	(Dibaei et al., 2020) (Khan et al., 2020)
Black hole	V2X	Cryptography	(Dibaei et al., 2020) (Khan et al., 2020)

through the electric charging systems and the plugging into the grid.

Finally, the in-vehicle communication networks can be attacked through the vehicle **infotainment system** which offers user-friendly functions and an integration with smartphone applications (Pan et al., 2017). They are systems combining information and entertainment through pairs applications where one is executed in-vehicle and the other one on an external device like a smartphone. Such systems are connected to the CAN bus which makes it an entry point to a malicious packet injection as demonstrated by Mazloom et al. (2016).

3.2. Communication Threatthreats

Connectivity to external entities complements the in-vehicle components to achieve the automation of the ACS. Such connectivity is built through multiple channels: radio (AM/FM/DAB/RFID), WIFI (IEEE 802.11), Bluetooth, cellular (3/4/5G), bidirectional communication (IEEE 802.11p, Dedicated Short-Range Communication (DSRC), Wireless Access in Vehicular Environments (WAVE)) and, in some cases, IoT networks (IEEE 802.15.4, Zigbee) (El-Rewini et al., 2020; Maple et al., 2019). With the presence of wireless connections, Vehicular Ad-hoc Network (VANET) can be spontaneously created among connected and moving vehicles (Lee and Atkison, 2020). Initially, such ad-hoc networks were connecting only vehicles leading to V2V communication mode. Although, with the increase of modern concepts, infrastructure and additional devices, V2I and V2X were required to assist the VANETs for data storage and data transmission for long distances (Lee and Atkison, 2020). Nevertheless, being hyper-connected by nature, ACS environment has to deal with additional cybersecurity breaches highlighted as communication attack vectors in this section and in Fig. 2.

3.2.1. Vehicle-to-vehicle

provides means for ACSs to connect to other vehicles to broadcast traffic conditions and share the predictions and information within the VANET range (Parkinson et al., 2017). V2V technology is mainly supported by DSRC and WiFi which raises the risk of security breaches (Elliott et al., 2019). Relying on the weaknesses of communication technologies, numerous attacks such as jamming, bogus information, sybil, impersonation and timing can be conducted (Bhargava et al., 2016; Dibaei et al., 2020; El-Rewini et al., 2020). Baqer and Krings demonstrated how the loss of messages on V2V due to jamming can make the vehicle invisible within the ad-hoc network (Baqer and Krings, 2019). Performed on wireless networks, bogus information attack occurs when incorrect information is transmitted pushing other vehicles to change their path while freeing the way for the attacker (El-Rewini et al., 2020). Gu et al. (2017) demonstrated a sybil attack which happens when a vehicle declares itself as multiple ones, either to create congestion or congestion-free routes. Furthermore, a timing attack takes place when a malicious vehicle adds time delay to a received message, then forward it back to other vehicles, causing accidents due to the non-real time inputs (Dibaei et al., 2020).

3.2.2. Vehicle-to-infrastructure

This communication is illustrated by the data exchange between on-board unit (OBU) (also called on-board equipment (OBE)) and road side unit (RSU) (El-Rewini et al., 2020). Located at the ACS, OBU sends and receives messages to RSUs using virtual machines (VM) as secure cloud connections (Elliott et al., 2019). Messages sent from OBU to RSU through VM (also called beacon messages) may contain the vehicle velocity, location and pseudonyms. Such messages can include Cooperative Awareness Messages (CAM), Decentralized Environmental Notification Messages (DENM) or Basic Safety Message (BSM) where CAM and DENM are mainly used in European standards while BSM is used in United States of America (USA) (Krontiris et al., 2020). However, if eavesdropped by an attacker, location information in DENM or vehicle information in CAM can be inferred leading to a mapping attack where location privacy leakage is occurring (Kang et al., 2016). By making an RSU unable to function, Maple et al. (2019) pointed out the risk of DOS attack, hardware tampering and disabling attack. Dibaei et al. added the risk of replay attacks over the communication with RSUs by repeating or delaying valid transmission data (Dibaei et al., 2020).

Furthermore, V2I embeds the communication between ACS and Trusted authorities (TA) systems (Petit and Shladover, 2015) which represent an additional surface attack. Initially, the TA role is to generate short term certificates and public/private keys to verify the exchanged traffic messages (Ali and Li, 2020). In a scenario of

an attack, invalid messages through fake certificates would lead the TA systems to failure to warn about a crash for example (Petit and Shladover, 2015).

3.2.3. Vehicle-to-everything

This communication mode wraps both V2I and V2V technologies and respectively the attacks risks. V2X also compasses cloud and edge servers communication in addition to any further devices or peripherals interacting with the vehicle such as smartphones, car keys or Bluetooth devices (Petit and Shladover, 2015). Vehicle-to-cloud (V2C) and Vehicle-to-pedestrian (V2P) are additional vehicle communications classifications highlighted by Lozano and Sanguino (2019) and considered as a part of V2X. Maple et al. (2019) described further attacks like DOS, black hole and MitM that can be conducted over the vehicular network through a cloud connection and edge servers. Pan et al. (2017) demonstrated a smartphone attack by connecting an Android mobile phone to the vehicular system and injecting malicious CAN data through Bluetooth connection.

3.3. Mitigation strategies

As ACSs' related threats have been identified in Sections 3.1 and 3.2, it is important to recognise existing defences and mitigation solutions against them. As described in Table 3, many researchers highlighted the advantages of redundancy and cryptography to countermeasure spoofing, sniffing, jamming, replaying, and tampering attacks (Bailey, 2018; Changalvala and Malik, 2019; Daimi and Saed, 2018; Khanam et al., 2020; Nguyen et al., 2015). Others focused on newer trends such as Blockchain (BC), Intrusion Detection System (IDS) and Machine and Deep Learning (MDL) to detect abnormal behaviour and, hence, circumvent the security challenges (Dibaei et al., 2020; El-Rewini et al., 2020; Gupta et al., 2020; Oham et al., 2021). Besides, classical prevention techniques such as firewalling and network segmenting remain essential to restrain the occurrence of jamming, DOS or MitM attacks over in-vehicle networks (Pesé et al., 2017) or cloud communications (Maple et al., 2019). By considering the advantages and disadvantages of each mitigation technique, the present work agrees on the requirement of adapting and combining multiple defences in addition to the consideration of the human factors to shield the ACSs.

3.3.1. Redundancy, fusion and randomisation

Anomalous sensor readings can be improved by sensor redundancy (Yan et al., 2016). In case of a GPS jamming, the combined data from other sensors, like LiDAR and RADAR, can cross-validate the initial measurement for the same parameter, maintain the vehicle navigation until the GPS signal is back and, therefore, discard the attack consequences (Van Wyk et al., 2020). Redundant cameras can also countermeasure the cameras' blinding attack. By multiplying the number of cameras and locating them in different points, the vehicle can continue operating even if one of the cameras is blinded (Parkinson et al., 2017). Petit and Shladover (2015) highlighted the advantages of redundancy as a mitigation solution to jamming, yet the additional equipment or processing for fusing data would certainly increase related costs and computations overhead.

Moreover, introducing randomness into RADAR, LiDAR and ultrasonic sensors would reduce the spoofing risk (Ren et al., 2020). Shin et al. (2017) assessed that by emitting signals in random instants, the attacker can no longer induce multiple fake dots.

3.3.2. Cryptography

In connected automated driving environment, encryption is a crucial strategy to ensure security and, thus, safety. On a vehicular network, the vehicle needs to be securely authenticated using key encryption algorithms to communicate with RSUs, OBUs and to get TA certifications (Dibaei et al., 2020). Symmetric Key Schemes (SKS) and Asymmetric Key Schemes (AKS) can assure secure authentication of the vehicle within the VANET and protect from attacks such as replay, sybil and impersonation (Dibaei et al., 2020). In SKS, which is also called secret-key encryption, it is assumed that the sender and receiver nodes share a single key that is used for both encryption and decryption (Mushtaq et al., 2017). Advanced Encryption Standard (AES), Data Encryption Standard (DES), Tiny Encryption Algorithm (TEA), International Data Encryption Algorithm (IDEA) are examples of SKS providing high security against attacks like MitM (Khanam et al., 2020). AKS also known as Public Key Cryptography (PKC) is an approach used to build secure communication between two or more nodes where the sender encrypts the message using the public key and the receiver decrypts it using his private key (Nguyen et al., 2015). The AKS include Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH) and Elliptic Curves Cryptography (ECC) which have been proven to strengthen the system again attacks like timing and eavesdropping (Khanam et al., 2020).

As discussed in Section 3.1.2, messages exchanged among ECUs are in general neither encrypted nor authenticated. Potential authentication techniques using Message Authentication Code (MAC) have been investigated to countermeasure attacks over the in-vehicle networks such as CAN (Tashiro et al., 2018) and LIN (Takahashi et al., 2017). Such solutions may employ SKS and AKS to authenticate the sender ECU, initiate the message exchange and let the receiver ECU detect the attack (El-Rewini et al., 2020). Nguyen et al. (2019) introduced quantum cryptography based on SKS to detect intrusions and secure the communication between ECUs and the CAN. Though, calculation time should be considered in order to limit the traffic overhead (Gupta et al., 2020; Tashiro et al., 2018).

Not limited to network attacks only, it has been showcased that cryptography reduces attacks on sensors and protects the ACS ports. Daimi and Saed (2018) suggested the replacement of regular sensors (like TPMS) with more performing ones which contain processing resources for authentication and encryption functionalities. Bailey (2018) demonstrated the efficiency of cryptography on limiting the GPS spoofing. El-Rewini et al. (2020) added that SKS and AKS would prevent from injecting malware through OBD-II, USB and electric charging ports.

Despite their advantages, encryption algorithms may cause latency and impact the network efficiency due to their computational complexity (Changalvala and Malik, 2019; Nguyen et al., 2015).

3.3.3. Blockchain

To reduce the implementation burden of cryptography, BC has been introduced as a promising defence which increases the authentication on the VANETs, in-vehicle communication and the accuracy of GPS positioning (Dibaei et al., 2020). BC is a distributed ledger technology made of connected data blocks which verify the state of component (like ECU for example) based on a decentralised consensus (Noh et al., 2020). In other words, as the blocks of data are protected by the consensus protocols, the distributed nature of the BC makes it difficult to conduct an attack (Chowdhury et al., 2019). Li et al. (2020) proved how their proposed blockchain-based GPS model provides accurate positioning data even in the case of a GPS spoofing or jamming. Oham et al. (2021) demonstrated the BC efficiency on monitoring the in-vehicle network and detecting attacks over it. Gupta et al. (2020) discusses the advantages of integrating BC to the CAV architecture by emphasising on how it countermeasures the limitations of cryptography within the driverless system.

3.3.4. Intrusion detection system and machine and deep learning

IDS has been judged as the most reliable countermeasure to VANET (Zhang and Zhu, 2018) and in-vehicle communication threats (El-Rewini et al., 2020). It aims to detect and isolate anomalies while monitoring the network traffic. The IDS can be deployed either by detecting predefined attacks through the signature-based detection techniques; or by distinguishing a behaviour change through the anomaly-based detection method (Ioulianou et al., 2018). The signature-based detection identifies the attack by comparing the attack case to a database of signatures of already known attacks (Ioulianou et al., 2018). The anomaly-based detection can incorporate machine learning methods to train itself on normal behaviours, then anything that is different from the expected cases will be detected as an attack (Dibaei et al., 2020). Wu et al. (2020) and Ali Alheeti and Mc Donald-Maier (2018) demonstrated the efficiency of the IDS over network attacks like DOS. Further research works extended the IDS to be collaborative and distributed within the VANET which enables knowledge sharing among vehicles while reducing storage and workload burden (Zhang and Zhu, 2018).

Multiple studies detected anomalous behaviour using MDL theories. Van Wyk et al. (2020) presented a real-time anomaly detection by combining a deep learning technique (Convolutional Neural Network (CNN)) with Kalman filtering (Śmieszek and Dobrzańska, 2015) which provides high accuracy for automated driving environment. The authors' generic framework was proved to detect anomalous behaviour originating internally from in-vehicle sensors, or externally from an OBU or/and an RSU. In addition, Kang and Kang (2016) demonstrated the efficiency of Deep Neural Network (DNN) in monitoring and detecting attacks over the CAN bus. Further researchers (Bezemskij et al., 2018; Sheehan et al., 2019) showcased the efficiency of their models based on Bayesian Network as a deep learning theory to monitor attacks from sensors. Khanam et al. (2020) assessed the advantages of additional MDL algorithms, in detecting network spoofing and DOS attacks within the IoT environment, such as Recurrent Neural Network (RNN), Artificial Neural Network (ANN), Deep Belief Network Network (DBN) and Support Vector Machine (SVM).

3.3.5. Software vulnerability detection

With the high risk of code intrinsic vulnerabilities on ECUs and any software embedded to the automated driving system, static and dynamic analyses, in addition to MDL methods have been mainly used for software vulnerability detection. Static analysers are used to check the program without executing it, while the dynamic techniques check the code during the program execution (Dibaei et al., 2020). Pattern matching, lexical analysis, parsing, control flow analysis and data flow analysis are examples of static methods providing short analysis time but with high false positive rate (Ferrara et al., 2021). On the other hand, fault injection, fuzzing and dynamic taint analysis illustrate dynamic analysis mechanisms granting higher accuracy but with a longer analysis time (Kim et al., 2016). However, static and dynamic analyses have been considered as traditional methods by considering their drawbacks and tend to be replaced by machine deep learning methods. Russell et al. (2019) and Li et al. (2019) trained the MDL algorithms and demonstrated their effectiveness on software vulnerability detection. Jeon et al. (2020) used CNN to detect new and variant malware within the IoT environment.

3.3.6. Further solutions supporting technical mitigation techniques

An indirect, but interesting defence to V2X cyber risks, would be the 5G new communication technology. It is true that 5G may inherit some of the 4G vulnerabilities as few specifications remain unchanged from the precedent protocol; though, it provides higher bandwidth which facilitates the encryption and authentication implementations without causing network latency (Chowdhury et al., 2019). Dibaei et al. (2020) added that the ultra-low latency and real-time response features of the 5G would enable real time warnings and attacks detection within the V2X environment. Nevertheless, Ahmad et al. (2019) warned about further known and unknown threats caused by the 5G that CAVs would have to cope with as additional threats.

In addition to technical solutions, human factors can contribute to build defences within the vehicular environment. Linkov et al. (2019) highlighted the fact that human behaviour during cyber attack should be taken into account when designing ACSs and when recruiting operators working on them. The authors added that cybersecurity can be improved by considering human factors such as workload, knowledge and training about cybersecurity risks. Operators who are informed about the cyber attacks risks and who had training on secure authentication and phishing would behave more securely.

Marksteiner and Ma (2019) assessed that testing is very important in the security development, though, it is mainly conducted by in-house pentesters, and their results depend on the human skills and the manufacturer budget. With the trend of minimising human intervention, researchers such as Chu and Lisitsa (2019); Johari et al. (2020) and Casola et al. (2018) introduced automated pentesting models within IoT and proved their efficiency on both code and network vulnerabilities. However, the authors approach is limited to known threats while powerful criminal cyber attacks took place usually over unknown vulnerabilities (Upstream Security, 2018).

Hence, automobile manufacturerss (OEMs) and the public transportation companies should take into consideration findings related to human factors while forming their ACSs' teams by emphasising on collaborators' cybersecurity risk knowledge and awareness.

To that end, the ACS's stakeholders should carefully deploy the accurate mitigation measures based on the embedded systems within the vehicle and the mini-buses connectivity modes supported by the VANET. Nevertheless, the countermeasures can not be limited to technical and human defences as organisational regulations can be combined to the aforementioned discussed solutions for an optimal vehicle shielding, as described in the following subsection.

3.4. Cybersecurity regulations

Cybersecurity should be considered while deploying every piece of hardware and software on the ACS to avoid the aforementioned threats. In addition to the technical countermeasures, governments, regulatory bodies and information systems institutions can contribute on building secure ACSs' environment. It has to be mentioned that there are not many mandatory legal frameworks incorporated in the legal systems in the field of cybersecurity, let alone in specific sectors such as transport. Though, many stakeholders including OEMs, regulatory bodies, IT and telecommunication suppliers, operators of ITS, and mobility service providers collaborate and establish new regulatory approaches, strategies and guidelines. In this section, we highlight global efforts, with a focus on Europe, in building cybersecurity legal frameworks and guidelines for the automated driving landscape as summarised in Table 4. The table highlights the regulations and their regulatory bodies, their locations and date of entry into force. The table also lists the regulations based on their types to be either a law (a mandatory act), guidance (a statement of advice pertaining to practice) or recommendation (a statement of practice) (Oxford English Dictionary, 2021).

Table 4
Cybersecurity regulations summary.

Regulatory body	Regulation	Regulation type	Country	Date
European Parliament and the Council of the EU	NIS Directive 1 (The European Parliament and the Council of the European Union, 2016a)	Law	EU	July 2016
	NIS Directive 2 (The European Parliament and the Council of the European Union, 2020)	Law	EU	January 2020
ENISA	Cyber security for Smart Cities (ENISA, 2015)	Guidance	EU	December 2015
	Cyber Security and Resilience of Smart Cars (ENISA, 2017)	Guidance	EU	December 2016
	Good Practices for Security of Smart Cars (ENISA, 2019)	Guidance	EU	November 2019
	Cybersecurity Stocktaking in the CAM(ENISA, 2020a)	Guidance	EU	November 2020
	Guidelines for Securing the IoT (ENISA, 2020b)	Guidance	EU	November 2020
JRC	Certificate Policy for Deployment and Operation of European C-ITS (European Commission, 2018)	Guidance	EU	December 2015
ENISA and JRC	Cybersecurity Challenges in the Uptake of AI in Autonomous Driving (ENISA, 2021)	Guidance	EU	February 2021
ACEA	Principles of Automobile Cybersecurity (European Automotive Manufacturers Association (ACEA), 2017)	Guidance	EU	September 2017
	Roadmap for the Deployment of Automated Driving in EU (European Automotive Manufacturers Association (ACEA), 2019)	Guidance	EU	December 2019
UK Government	The Pathway to Driverless Cars (Department for Transport, 2015)	Guidance	UK	February 2015
	The Key Principles of Vehicle Cyber security for CAVs (HM Government, 2017)	Guidance	UK	August 2017
	Automated and Electric Vehicles Act 2018 (UK-Government, 2018)	Law	UK	July 2018
DOT	Ensuring American Leadership in Automated vehicle Technologies 4.0 (National Science and Technology Council and the United States Department of Transportation, 2020)	Guidance	USA	January 2020
NHTSA	Automated Driving Automated Driving Systems A vision for Safety (NHTSA, 2017; 2021)	Guidance	USA	2016, 2020
Auto-ISAC	Best Practice Guide (Auto-ISAC, 2022)	Guidance	USA	July 2016
IPA	Approaches for Vehicle Information Security (Kobayashi et al., 2013)	Guidance	Japan	August 2013
ITU-T	X.1371: Security Threats to Connected Vehicles (ITU-T, 2020a)	Recommendation	Intergovernmental	May 2020
	X.1372: Security Guidelines for V2X (ITU-T, 2020b)	Recommendation	Intergovernmental	March 2020
	X.1373: Secure Software Update Capability for ITS Communication Devices (ITU-T, 2017)	Recommendation	Intergovernmental	March 2017
	X.1374: Security Requirements for External Interfaces and Devices with Vehicle Access Capability (ITU-T, 2020c)	Recommendation	Intergovernmental	October 2020
	X.1375: Guidelines for an Intrusion Detection System for In-Vehicle Networks (ITU-T, 2020d)	Recommendation	Intergovernmental	October 2020
	X.1376: Security-related Misbehaviour Detection Mechanism using Big Data for Connected Vehicles (ITU-T, 2021b)	Recommendation	Intergovernmental	January 2021
UNECE	UN R155 (UNECE, 2020a) UN R156 (UNECE, 2020b)	Law	Intergovernmental	January 2021

3.4.1. European union

CAVs stakeholders have been encouraging "Regulatory Sandboxes" and "Living Labs", where new technologies are tested accordingly to the legal requirements by predicting undesired consequences and through a learning-by-doing approach (Costantini et al., 2020). C-ROADS (C-Roads, 2021) platform illustrates such labs in Europe supporting on testing and implementing the European Strategy on Cooperative Intelligent Transport Systems (C-ITS) since 2016. Furthermore, the Connected, Automated and Autonomous Mobility (CCAM) single platform was launched in 2019 by the European Commission for supporting on open road testing including activities related to connectivity, digital infrastructure, cybersecurity and access to in-vehicle data (European Commissopn, 2022; ENISA, 2020a; 2021).

Based on such labs' findings, the first European Union (EU)-wide law on cybersecurity, the Directive (EU) 2016/1148 (The European Parliament and the Council of the European Union, 2016a), known as "Network and Information Security (NIS) Directive", came into force. This directive defines measures for a high level of network security and information systems across the EU. The "NIS Directive" covers the vehicles' cybersecurity issues under its generic security scope for preventing and minimising the incidents and attacks impact. In December 2020, new proposals were published with an updated version called "NIS 2" (The European Parliament and the Council of the European Union, 2020). Both directives call the operators of essential services and the digital services providers to take the appropriate and proportionate technical and organisational measures to manage the risks posed to the security of information systems.

More specific to the road transport sector, European Union Agency for Cybersecurity (ENISA) came up with guidelines on implementing the NIS Directive. ENISA published multiple reports depicting the key challenges and requirements for smart cars and smart cities from cybersecurity perspectives (ENISA, 2015; 2017; 2019; 2020a; 2020b). Among the European Commission's efforts, the Joint Research Centre (JRC) has set up a security Public Key Infrastructure (PKI) model for a safe V2X communication (European Commission, 2018). ENISA and JRC published their latest report in February 2021 discussing Artificial Intelligence (AI) specific cybersecurity challenges related to automated driving environment (ENISA, 2021).

By taking into account ENISA's recommendations, the European Automobile Manufacturers Association (ACEA) identified key principles for cybersecurity protection against attacks on CAVs emphasising on implementing cybersecurity requirements through every stage of the vehicle development lifecycle (European Automotive Manufacturers Association (ACEA), 2017). In 2019, ACEA published a roadmap for the deployment of automated driving in the EU spurring OEMs to self-audit, testing, and deploying incident response plans (European Automotive Manufacturers Association (ACEA), 2019).

3.4.2. United Kingdom

According to KPMG's CAV readiness index, the United Kingdom (UK) was ranked as number one in the world in 2020 for cybersecurity in terms of regulations efforts (KPMG, 2020). In 2015, the Department for Transport in the UK published "The Pathway to Driverless Cars" as good to have practices, on automated driving, highlighting cybersecurity risks and privacy issues (Department for Transport, 2015). In 2017, the UK government presented the eight key cybersecurity principles for CAVs pointing out the importance of organisation security management, system resiliency and risk assessment throughout the vehicle lifecycle using a defence-in-depth approach (HM Government, 2017). In 2018, the UK's first legislation on CAVs titled "Automated and Electric Vehicles Act 2018" came into force (UK-Government, 2018). Considering the quick progress of the driverless ecosystem, the British government launched a second consultation on exploring the regulation of secure ACSs (The UK Centre for Connected and Autonomous Vehicles, 2020). Furthermore, the UK government's efforts contributed to the development of the British Standards Institution (BSI)'s standards discussed later in Section 5.6.

3.4.3. United States of America

In January 2020, the Department of Transport (DOT) shared a report titled "Ensuring American Leadership in Automated vehicle Technologies 4.0" (National Science and Technology Council and the United States Department of Transportation, 2020). From the report, the USA government highlighted their efforts with different stakeholders to ensure security and cybersecurity mechanisms through successful prevention, mitigation and investigation of security threats targeting the driverless ecosystem. The report further assessed the NHTSA mission on developing and updating cybersecurity best practices. Since 2016, the NHTSA shared a voluntary guidance to strengthen motor vehicle cybersecurity and protect the electronic systems from potential attacks, which was updated in 2020 (NHTSA, 2017; Taeihagh and Lim, 2018). The updated guidance consists of general cybersecurity requirements like vulnerabilities reporting, incident monitoring and responses in addition to self auditing. The NHTSA guidance includes also technical cybersecurity best practices like the implementation of PKI certifications, encryption keys and secure software updates (NHTSA, 2021). Besides, Automotive Information Sharing and Analysis Center (Auto-ISAC) is an alliance of global automakers who joined their forces to develop and upgrade a series of best practices with the evolving of CAVs ecosystem. Similarly to NHTSA, the Auto-ISAC best practices focus on cybersecurity general requirements like threat detection, monitoring and response in addition to security development lifecycle considerations Auto-ISAC (2022).

3.4.4. Japan

In 2013, the Japanese Information-Technology Promotion Agency (IPA), published a guidance paper where the in-vehicle threats and countermeasures are mapped (Kobayashi et al., 2013). The publication includes also a checklist for vehicular developers on how to mitigate particular attacks like DOS. The IPA recommendations are presented through a mapping of four security levels to the automotive system lifecycle including management, planning, development, operation and disposal. Even being dated, the IPA guide is much applicable and serves as a background to the Japanese guideline, JASO TP-15002, published in 2016 by the Society of Automotive Engineers of Japan (JSAE). JASO TP-15002 recommends a security analysis process of five phases focusing on security evaluation and major security risks mitigation (Kawanishi et al., 2019). Further notable collaborations between JSAE and Japan Automobile Manufacturers Association (JAMA) led to the creation of the Japan Automotive Software Platform and Architecture (JASPAR) (JasPar, 2021) and a Japanese Auto-ISAC J-Auto-ISAC (2022) focusing on local specific cybersecurity and information sharing issues related to ECUs and in-vehicle networks (METI, 2018).

3.4.5. Intergovernmental recommendations

In an intergovernmental context, the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) (ITU-T, 2021a) from the United Nations agency, has a working group focusing on developing security recommendations related to CAVs. Since 2017, their recommendations series (X.1371 to X.1376) cover security threats definition, security guidelines for V2X, specification of secure software update procedure for ITS's devices, guidelines for intrusion and misbehaviour detection as presented in details in Table 4.

Furthermore, United Nations Economic Commission for Europe (UNECE) working party WP29 adopted two new regulations on uniform provisions concerning the approval of CAVs with regards to cybersecurity and software update management systems (Bonichon et al., 2019). The regulations known as "UN R155" (UNECE, 2020a) and "UN R156" (UNECE, 2020b) were adopted in June 2020 and came into force from January 2021 to offer a practical and holistic approach to automotive cybersecurity. The two regulations cover the cybersecurity risk management, security by design, security incidents detection and mitigation, and secure software updates over the CAV lifecycle including development, production and post-production (Suh, 2020). Among the two regulations requirements, certificate of compliance for software update management systems and Cybersecurity Management System (CSMS) has become recommended for vehicles with level three onward (according to the SAE automation classification) and for three years renewal (GRVA UNECE, 2020; Schmittner et al., 2020).

3.5. Cybersecurity summary

To answer the RQ1, the present section provided a systematic categorisation of cybersecurity threats. Two main vectors were identified: in-vehicle, where the vehicle sensors and the in-vehicle communication attack surfaces were depicted; and external communication threats where the potential VANET's vulnerabilities are discussed. Spoofing and jamming were described as the most likely attacks to occur impacting several in-vehicle sensors. Even minor threats leading to non-accurate positioning or incorrect vi-

sion can make the vehicle perceive non-existing obstacles or hit disbelieved surroundings. Such consequences would definitely impact the safety and the acceptance of the ACS as a new public transportation mode. Regarding communication threats, either conducted directly or remotely, DOS and malware injection were assessed as the most destructive attacks that can be fatal in highly connected environments. Additionally, it is true that the more connections are built with the vehicle's external environment, the more sophisticated are the services provided by the ACS. However, more risks and attack surfaces have to be considered with the increase of the mini-buses' connections.

Several countermeasures were discussed and grouped into technical and legal mitigation strategies. From the technical perspective, redundancy, fusion and randomisation were recommended to cross-validate the data collected from the sensors and discard any malicious inputs. Moreover, the strength of cryptography was showcased against network attacks, in-vehicle or VANET communication's threats. Though, such mitigation solutions require additional equipment and involve computational overhead. As a matter of fact, we discussed more lightweighted countermeasures such as BC which reduces the implementation burden. Besides, as we believe that risk mitigation is not pertinent only until the occurrence of a cyberattack, this section also discussed monitoring and attack detection tools such as MDL.

From the legal perspective, the NIS directives represent the unique cybersecurity text laws in Europe even if they are applicable to all IT fields. More specific to CAV, the R155 from UN-ECE requires the implementation of the CSMS certification for all vehicles starting from SAE level three. It is true that such certification provides more control to the vehicle type approval process, although it remains generic as it is relevant to levels three, four and five of automation where safety and security risks are not comparable. Furthermore, ENISA and JRC represent good practices to follow for deploying CAVs in Europe. Similarly, the other cited institutions and regulators discussed recommendations with interesting security-by-design approaches. However, to the best of our knowledge, there is no formal published regulation dedicated to ACS which require a combination of the existing text laws and recommendations and an adaptation of technical solutions based on the vehicle nature and its connectivity maturity.

Consequently, the human presence has a crucial role on both mitigating and reacting to a cyber threat within the ACS landscape. By considering an ACS, of SAE level 4 of automation, multiple fatal situations can be avoided by a well trained operator aboard. Taking a case of a simple laser pulse attack where the vehicle can be blinded, the operator can take over and correct the vehicle navigation. Nevertheless, on an ACS of level 5 of automation, the vehicle decision making units must have the accurate mitigation strategies in place and run on a fail-safe mode to assure security and safety accordingly.

To that end, RQ3 has been partially answered through the review of technical and legal strategies mitigating cybersecurity threats. Apart from security concerns, data privacy represents another challenge to tackle within deploying ACSs. It is conspicuous that in the automated driving ecosystem, some cybersecurity attacks embed privacy leakage risks too. To complement the answer for RQ3, the following section covers data privacy concerns by identifying related risks, technical mitigation strategies and relevant personal data protection regulations.

4. Data privacy

With their hyper-connected nature, the ACS generates data permanently and spawns multiple challenges to their users' fundamental rights and to the protection of personal data and privacy. The shuttle's sensors, cameras, in-vehicle systems, its V2X communication and eventual embedded MaaS platforms, produce huge amounts of data, most of which is considered as personal data such as vehicle's location, video/audio surveillance and passengers' identities and positions. This practically means that personal data can be received by an unrestricted data controllers (recipients), whose intentions and technological capacity are not, and cannot be known to the data subject (users) (Krontiris et al., 2020). Such situation creates concerns about the transparency, the proportionality and the necessity of data processing which requires higher level of personal data controls (Article 29 Data Protection Working Party, 2017). Moreover, being a part of the public transport system, ACSs may have more data controllers than CAVs, and hence further potential personal data leakage risks (Ainsalu et al., 2018; Lim and Taeihagh, 2018).

The article 4 from the General Data Protection Regulation (GDPR) defines the data processing impacting personal privacy to be: data collecting, recording, organising, structuring, storing, adapting, alternating, retrieving, consulting, using, transmitting, disseminating, aligning, combining, restricting, erasing and/or destructing (The European Parliament and the Council of the European Union, 2016b). As a matter of fact, by processing the data, the personal information can be exposed to various threats which vary from intentional criminal breaches to economical and social purposes (Karnouskos and Kerschbaum, 2018; Parkinson et al., 2017).

Criminal threats are illustrated as intrusions, in-vehicle thieves' attacks, tracking attacks or vehicle behaviour's manipulation like attacks discussed on Section 3. On the other hand, data can be processed for social profiling, improving the commercial services through LBS/ MaaS or tailored advertising and hence generating social and economic benefits (Lim and Taeihagh, 2018). It can also help disabled people, elderly and young kids to be followed by their relatives (Collingwood, 2017). In addition, collected data can contribute to the smartness of the city as it can reveal real time information on traffic, road condition and the CO_2 emission (Karnouskos and Kerschbaum, 2018). This non-criminal intention remains harmless and very important for the vehicle integrity; though, legal rights and data controllers have to be transparent to data subjects for any required data processing (Parkinson et al., 2017).

4.1. Technical mitigation solutions

Despite the intention, personal data recorded from ACSs has to be kept anonymous and encrypted wherever transmitted and securely stored. Cryptography and secure computation have been discussed in the literature as key technical solutions for preserving personal data and location privacy. Statistical and machine learning theories have been investigated as techniques that would preserve the data confidentiality and anonymity without ownership restrictions or usage agreements.

4.1.1. Cryptography for personal data protection

As discussed in Section 3.2.2, privacy cannot be bypassed in VANETs as the vehicle identity and location are shared with RSUs, OBUs and TAs. Conditional Privacy-Preserving Authentication (CPPA) protocols have been introduced to make the TA as the only partner who can extract the real vehicle identity which may be hidden using signed messages or vehicle's pseudonyms (Manivannan et al., 2020). Lu et al. (2019) assessed that the anonymity is assured by using PKI based authentication, identity based signature, certificateless signature or group signature as cryptography mechanisms. Based on AKS, Dibaei et al. (2020) presented further privacy preserving protocols such as Group Signature and Identity-based Signature (GSIS) and Privacy-Preserving Group Communication Scheme for VANETs

(PPGCV) providing robust privacy protection within the vehicular network. Though, as any authentication based schemes, computations and storage burden should be considered. Multiple researchers (He et al., 2015; Karati et al., 2018; Wang et al., 2016a; Wu et al., 2017) have introduced upgraded CPPA protocols and lightweight algorithms which guarantee privacy requirements with less computational and storage costs.

Additionally, encryption algorithms have been adapted for multimedia data to protect visual personal data. In video surveillance context, Asghar et al. (2019) defined the encryption approach to be the process of translating, completely or partially, plaintext to ciphertext using SKS and AKS. Standard ciphers like AES were initially used for their level of security, though more specific video encryption and lightweight algorithms (Duong-Ngoc et al., 2020; Muhammad et al., 2018; Zarouk and Souici, 2013), came afterwards to adhere the multimedia requirements. Moreover, encryption theories have been combined to redaction-based techniques like scrambling to localise and encrypt recorded personal faces, however such algorithms require more storage considerations as they increase the video size (Liu et al., 2018).

Among cryptography solutions, Zero Knowledge Theory (ZKP) is a promising protocol that is based on an exchange of messages between the prover and the verifier where the prover has a secret but does not reveal information about it. However, the prover should provide more information about his secret to establish the trust with the verifier (Wan et al., 2019). Theoretically, the protocol is powerful and efficient for cryptographic applications, but the iterations for finding required proofs remain unpractical and costly in real-world use. The ZKP theory was improved in Wan et al. (2019) and Almuhammadi and Neuman (2005) by reducing the number of iterations rounds and hence reducing its costs; though, the additional collected information by the verifier presents a risk for a future data leakage and again impacts the individual's privacy.

4.1.2. Location privacy protection

Lu et al. (2019) defined the location privacy risk to be the ability to link an entity's spacial information to its identity. The vehicle ID, timestamp and GPS coordinates that are transmitted within CAM and DENM messages (also referred to as beacon messages Veitas and Delaere, 2018), are mainly used for collision avoidance, transport services (MaaS), or customised LBS. However, if eavesdropped, beacon messages may be reused for malicious vehicle tracking, or to infer future vehicle movements based on its past locations (Asuquo et al., 2018). Takbiri et al. (2017) classified location protection mechanisms into two main groups and recommended their combination: anonymisation-based techniques where the identity is concealed and obfuscation-based schemes where the location is perturbed.

In anonymisation-based schemes, pseudonyms replace the vehicle real identity and are changed periodically per the vehicle speed and direction (Lu et al., 2019). Such schemes are illustrated through Mix-zones or Silent approaches where beacon messages can't be easily eavesdropped as vehicles change their pseudonyms frequently (Asuquo et al., 2018). Furthermore, Kang et al. (2016) introduced pseudonym-changing synchronisation schemes to prevent from location leakage while communicating with RSUs using random identifiers.

Obfuscation-based schemes are used to make the unauthorised tracking difficult by decreasing the accuracy of location information on purpose (Lu et al., 2019). Such schemes aim to perturb position and beacon frequency to increase the tracker confusion (Asuquo et al., 2018). Lim et al. (2017) demonstrated an obfuscation-based solution to confuse the tracker while the location privacy and the quality of LBS are preserved.

4.1.3. Statistical and machine learning protocols

Differential Privacy (Dwork and Roth, 2013) and Randomised Response (Wang et al., 2016b) techniques illustrate the promise of learning useful information about a population while the individuals privacy is conserved. By adding random noise to a set of data before learning from it, private inputs get hidden without impacting the result accuracy (Nayak et al., 2016). Additionally, the haystack privacy policy (Joy and Gerla, 2017) is another efficient method preserving privacy using almost the same principle as Differential Privacy and Randomised Response, but with larger data owners participation. Applied to vehicular data, Zhang and Zhu (2018) demonstrated a collaborative IDS on VANETs based on differential privacy while Joy and Gerla (2017) showcased the haystack privacy theory over CAV's collected data. They assessed that such algorithms represent a new vision for privacy protection over vehicular training data sets.

Given the aforementioned theories, privacy can be technically assured. However, the presented techniques won't be enough if ownership rights and legislation are not well defined while using public ACSs. In the discussion that follows, the focus is on how individuals' privacy can be protected from legal perspectives, and what are the existing regulations controlling data governance to enhance privacy and confidentiality on ACSs without impacting their benefits.

4.2. Data privacy regulation

Personal data protection regulations govern the processing, usage, storage, and sharing of personal data. Those regulations have been identified also to give the opportunity to data subjects, as passengers in the case of ACSs, to consent or not to the use of their own personal information and to decide about the type of data and its relevant processing (Glancy, 2012). This section sheds light on the existing mandatory data privacy regulations (hard laws) in addition to existing soft law guidelines supporting the protection of personal information generated within the automated driving landscape as summarised in Table 5.

4.2.1. The European union regulations and initiatives

In the EU, the **Data Protection Working Group 4 (WG4)** of C-ITS analysed multiple options to deem lawful processing of personal data (The Data Protection WG of the C-ITS Platform, 2016). In the final report published in 2016, the WG4 assessed that the exchanged CAM and DENM (beacon messages) within the V2X environment, is personal data requiring legal and technical protection. Additionally, the WG4 highlighted the challenges on implementing the consent in practice (Krontiris et al., 2020).

Besides, the **Article 29 Working Party (WP29)** did further analysis on data privacy protection (Article 29 Data Protection Working Party, 2017). In 2017, the WP29 provided guidance on the processing of personal data in the context of C-ITS. Thereafter, the European Data Protection Board (EDPB), successor of WP29, published initially in January 2020 and updated in March 2021, guidelines highlighting privacy and data protection risks. The EDPB guide includes also recommendations on data protection by design and by default, in addition to a simulation of five illustrations of data processing within CAV environment (European Data Protection Board, 2020; European data Protection Board, 2021). Moreover, the guidelines focus on consent as the legal basis for processing personal data inside the vehicle and through V2X communications (Krontiris et al., 2020). The EDPB guidance incorporates both e-Privacy directive and GDPR (European Data Protection Board, 2020). Although the guidelines are referring to the processing of personal data in relation to the non-professional use of CAVs, it could be perceived as a valuable guide for the protection of personal data for the public ACSs as well (ACEA, 2020).

Table 5
Data privacy regulations summary.

Type	European	Global[a]
Hard Laws	e-Privacy Directive (European Parliament and the Council of the European Union, 2002) GDPR (The European Parliament and the Council of the European Union, 2016b)	S.2182 SPY Car (Congress, 2019) H.R.3388 Self Drive (Congress, 2017) Australia Policy Paper (Australia, 2018) APPI (Personal Information Protection Commission, 2016)
Soft Laws / Regulator Bodies	WG4 (The Data Protection WG of the C-ITS Platform, 2016) EDPB (European Data Protection Board, 2020; European data Protection Board, 2021) GAIA-X (GAIA-X, 2022) Data for Road Safety (Data for Road Safety, 2021)	UNECE (UNECE, 2016; 2019) ICDPPC (ICDPPC, 2017) IWGDPT (IWGDPT, 2018)

[a] Limited to the cited countries in the present section.

The **e-Privacy Directive** (European Parliament and the Council of the European Union, 2002) represents a mandatory standard applying to electronic communication networks and entities reading from a terminal equipment within the European Economic Area (EEA). Such terminal equipment can be identified as the ACS per the EDPB definition (European Data Protection Board, 2020). The e-Privacy directive sets rules of tracking technologies, and presents fragmentation of legislation with an alignment to GDPR (Veitas and Delaere, 2018).

The Regulation (EU) 2016/679 ("General Data Protection Regulation" GDPR The European Parliament and the Council of the European Union, 2016b) replaced the directive 95/46/EC and contains provisions and requirements related to the processing of personal data in order to protect fundamental rights and freedoms of natural persons, the data subjects, and in particular their fundamental right to privacy and the protection of personal data. Inter alia, the GDPR identifies new data governance roles (data subjects, data controller, data processor and data protection officer) and introduces the accountability principle as the cornerstone of personal data processing.

According to the GDPR, the data should be processed lawfully and fairly under transparency and minimisation principles (art. 5 and 6) GDPR) (The European Parliament and the Council of the European Union, 2016b). In addition, the GDPR attributes rights to data subjects as well as obligations for the data controllers and data processors. The GDPR emphasises on data subjects rights which vary from rights to transparent information access (art. 12, 13 and 15), right to rectification (art. 16), right to erasure (art. 17), right to restriction of processing (art. 18), to right to be notified in case of data breaches occurrence (art 33 and 34). Any failure of the data controller and the data processor to comply with these principles and not to protect the rights of data subjects, may result in fines (article 83). Applied to the ACS ecosystem, the shuttle passengers and operators (if any) should be informed, with transparency, and provide their consent about all the processing applicable to their personal data in addition to being notified, under circumstances, when cyber incidents take place and their personal information may be leaked (or breached).

Moreover, the GDPR come up with technical and security commitments that should be considered by data controllers to guarantee data integrity and confidentiality. Articles 25 and 32 introduce the concepts of Privacy by Design and by Default requiring the implementation of risk management mechanisms and appropriate mitigation techniques such as encryption, pseudonymisation and data minimisation procedures from the outset (The European Parliament and the Council of the European Union, 2016b). The GDPR also recommends a data protection impact assessment (DPIA) as a useful practice within the design phase as detailed in articles 35 and 36 (European data Protection Board, 2021). As far as the processing concerns personal data, the GDPR and the e-Privacy Directive are considered as the main regulations in the EU to protect individuals' data within any deployed technology (European Data Protection Board, 2019).

Furthermore, based on GDPR and ePrivacy regulations, new initiatives and projects have emerged in the EU. One is **GAIA-X** (Fabian Biegel et al., 2020) which has been merging to increase data transparency and user trust. GAIA-X was launched in 2019 by stakeholders from business, politics and science fields to provide proposals on data protection rules and architecture standards in many areas including mobility and smart cities (Federal Ministry for Economic Affairs and Energy, 2020). **Data for Road Safety** is another initiative pushing for trustful and legal smart data exchange in the EU (Data for Road Safety, 2021). Data for Road Safety discusses connected vehicles of all automation levels and gathers partners from European Commission, industry, and governments to reach cooperative, trustworthy and free of charge vehicles data exchange with respect to the European regulations.

4.2.2. International initiatives

Not limited to the EU, some governments have either enacted laws on the protection of personal data or published guidelines that provide useful recommendations addressing privacy concerns in the automated driving environment. As CAVs had started entering the market, some countries (e.g. USA and Australia) have included automated driving concerns to their data protection regulations, while others (e.g. Japan) are still adjusting the broad laws that are not specific to driverless ecosystem, though applicable to the protection of personal data or privacy (Costantini et al., 2020; Lim and Taeihagh, 2018; Taeihagh and Lim, 2018). To illustrate, the **USA** government published dedicated acts for highly automated vehicles in a wide scope including ACSs. The S.2182 SPY Car (Congress, 2019) and the H.R.3388 Self Drive (Congress, 2017) Acts oblige OEM to develop written privacy plans prior to offering or importing CAVs. The acts highlighted that the privacy plan must be developed with respect to the collection, use, sharing and storage of personal data. Within the privacy plan, the vehicle passengers should be notified about the privacy policy unless the personal data is anonymised or encrypted. Similarly, **Australia** (Australia, 2018) published their dedicated regulations on protecting personal data within the automated driving environment. On the other hand, in **Japan**, Act on the Protection of Personal Information (APPI) (Personal Information Protection Commission, 2016) is the main data protection law but with a broad scope. The regulation came into force in May 2017 addressing the individual's information standalone or comprised with other data enabling the inference of the personal information which makes the law applicable to CAVs environment. According to articles 82 to 85 of the APPI, any violation of the act would lead to fines or imprisonment.

4.2.3. Intergovernmental initiatives

Additionally, at an intergovernmental level, the **UNECE** with its 56 governments as member states, made noteworthy efforts regarding the protection of personal data within CAVs environment. In 2016, the Informal Working Group on Intelligent Transport Systems and Automated Driving published guidelines proposal on cybersecurity and data protection (UNECE, 2016). The guidelines emphasises on data protection by default and by design. The report also assessed that data processing systems installed within an automated vehicle have to be data protection friendly. In 2019, UNECE published a framework document on CAVs where they identified the key principles of safety and security including Data Storage System for Automated Driving vehicles (DSSAD) (UNECE, 2019). The purpose of DSSAD is to establish legal data processing within a crash investigation context with respect of the national and regional data protection laws.

Furthermore, annual forums and international conferences contribute to setting the data privacy regulations for the driverless environment. In 2017, the **International Conference of Data Protection and Privacy Commissioners (ICDPPC)** adopted a high level resolution on CAVs where regulation bodies and OEMs were called to adopt privacy by design and privacy by default at every stage of the vehicle's devices and services development (ICDPPC, 2017). In a more detailed report, **International Working Group for Personal Data Protection in Telecommunications (IWGDPT)** adopted a working paper on CAVs discussing the type of data to be protected and recommendations to the multiple stakeholders (IWGDPT, 2018). The IWGDPT working paper also listed the privacy risks to be: lack of transparency, unlawful processing, unauthorised secondary use, excessive collection, lack of control, inadequate security, and lack of accountability.

4.3. Data privacy summary

To cover multitude nuances of RQ3 in this section, we investigated and identified the key privacy preserving theories that are commonly used in general IT contexts and applied them to the ACS scope. We identified relevant cryptography protocols to assure authentication of vehicular information, or hide visual data within the mini-buses cameras' recordings. Other powerful protocols anonymising personal identities or obfuscating vehicles' locations were discussed respectively. Such policies are very promising and highly recommended if not obliged by the discussed hard laws such as the GDPR.

Though, such mechanisms remain vulnerable to re-identification risks that can lead to easily infer or predict individuals and/or location attributes (Cormode, 2011; Kawamoto and Murakami, 2018). In other words, machine learning techniques implementing anonymisation requirements, such as Differential Privacy, Randomised Response and haystack privacy, as cited in Section 4.1, allow to recognise a person from mining non-personal inputs or by combining multiple data sets. With such a gap between technical implementations and legal provisions, the strict deployment of regulations may fall short in some real world situations. Hence, the application of a legislation has to be adapted to the context and type of data which can vary within the processing and the eventual reverse engineering technologies.

To conclude, and as an answer to RQ2, it is true that the deployment of the most pointed privacy preserving theories and the existing laws and regulations certainly increases data transparency and guarantees lawful processing. However, the de-anonymisation risk is never zero and personal data can still be somehow consumed and generate benefits for data controllers and third parties.

A more appropriate approach to overcome such shortcomings is to consider any technical mitigation technique or legal text on a case-by-case basis and/or as cooperative guidelines built by data controllers, policy makers, ACS' stakeholders and standardisation bodies that should be frequently updated to cope with the ACS evolving technologies. The following section presents standards and standardisation bodies' efforts on protecting the vehicular ecosystem from cybersecurity and data privacy breaches.

5. Standards

As in the automotive sector, ACSs stakeholders have been collaborating with standardisation bodies to build up measures and processes addressing security and privacy challenges. According to ENISA (ENISA, 2020a) relevant standards can be classified into three groups: Automotive where mainly ISO, SAE and Automotive Open System Architecture (AUTOSAR) have identified security framework and road maps over the in-vehicle components. The second group is the cooperative communication where ETSI working groups have outlined technical specifications on ITS. Finally, the third one is the generic cybersecurity group combining ISO and International Electronical Commission (IEC) collaborations. Beyond ENISA's classification, noteworthy efforts from other standardisation bodies such as European Committee for Standardization (CEN)-European Committee for Electronical Standardisation (CENELEC), BSI, and World Wide Web Consortium (W3C) are investigated and reviewed in this section as summarised in Table 6.

5.1. International organization for standardization (ISO)

ISO standards can be generic and transverse but still relevant to vehicular environment. The ISO 9001 (ISO, 2015), covering quality management requirements, can be relevant to any organisation regardless its services or products. In collaboration with IEC, the ISO/IEC 27K standards series (ISO, 2018a) came up to address information security and risk management controls. For more cybersecurity focused standards, there are the ISO/IEC 15408 (ISO, 2022), ISO/IEC 18045 (ISO, 2014) and ISO 20077/78 (ISO, 2018b; 2019a) which present general cybersecurity processes recommendations and computer security certifications. Additionally, ISO/IEC 20243 (ISO, 2018d) aims to reduce the risks related to malicious hardware or software. ISO standards embed also generic road vehicle safety requirements like ISO/PAS 21,448 (which will be replaced by ISO/DIS 21448) (ISO, 2019b), ISO 26262 (ISO, 2018c) and the last ISO/CD 24089 (ISO, 2021e) which is under development to discuss specifications for the vehicles' software updates.

To incorporate cybersecurity considerations in the vehicle environment, the ISO/TC22 working group joined their efforts to SAE and established the ISO/SAE 21434 (ISO, 2021h). The ISO/SAE 21,434 is a descendent of SAE J3061 which sets high level guidelines of cybersecurity approaches based on a life-cycle framework definition (Schmittner et al., 2016). Based on the SAE J3061, ISO/SAE 21,434 aims to achieve a common understanding of security by design over the entire supply chain in order to reduce the potential cybersecurity threats. ISO/SAE 21,434 covers also risk management requirements by referring to the generic ISO 3100 (Schoitsch and Schmittner, 2020). Nevertheless, the standard draft has been criticised by Macher et al. (2020) as being ambiguous since processes are described at a high level without prescribing specific technologies to countermeasure cybersecurity threats on the CAVs' environment. As further efforts from the ISO/TC22, ISO/SAE PAS 22,736 (ISO/TC22, 2021) came to update the taxonomy of the six levels of automation that was initially defined in SAE J3061. To that end, other standards such as ISO/DPAS 5112 might provide more visibility on automotive cybersecurity auditing (ISO, 2021b).

In the context of ITS, ISO founded ISO/TC 204 working groups who have been developing standards supporting the integration

Table 6
Standards summary.

S.Body	Standard ID	Scope	Description	Status
ISO	ISO 9001 (ISO, 2015)	Generic	Quality management systems	Published
	ISO 27K (ISO, 2018a)	Generic	Information security and risk management controls	Published
	ISO/IEC 15408 (ISO, 2022)	Cybersecurity	Evaluation criteria for IT security	Published
	ISO/IEC 18045 (ISO, 2014)	Cybersecurity	Methodology for IT security	Published
	ISO/IEC 20077 (ISO, 2018b)	Vehicle Cybersecurity	Extended vehicle communication	Published
	ISO/IEC 20078 (ISO, 2019a)	Vehicle Cybersecurity	Extended vehicle web services	Published
	ISO/IEC 20243 (ISO, 2018d)	Cybersecurity	Threats related to malicious hardware or software	Published
	ISO/PAS 21448 (ISO, 2019b)	Road vehicle safety	Safety of the intended functionality	Published
	ISO 26262 (ISO, 2018c)	Road vehicle safety	Functional Safety	Published
	ISO/CD 24089 (ISO, 2021e)	Vehicle software update	Vehicle software update	Under development
	ISO/SAE 21434 (ISO, 2021h)	Vehicle Cybersecurity	Cybersecurity engineering	Published
	ISO/SAE PAS 22736 (ISO/TC22, 2021)	ITS	Taxonomy and definitions for automation systems	Published
	ISO/DPAS 5112 (ISO, 2021b)	CAV's Audit	Guidelines for auditing cybersecurity engineering	Under development
	ISO/TS 21177 (ISO, 2019c)	ITS	Security and authenticity requirements for V2X	Published
	ISO 22737 (ISO, 2021c)	ACS	Low-speed automated driving systems for predefined routes	Published
	ISO 24014 (ISO, 2021a)	Public Transport	Interoperable fare management system	Published
	ISO/AWI 21734 (ISO, 2021d)	Automated driving buses	Connectivity and safety functions	Under development
	ISO/AWI TR 23254 (ISO, 2021f)	ITS	CAVs' architecture	Under development
	ISO/AWI TS 22726 (ISO, 2021g)	ITS	Dynamic data and map database specification for CAVs	Under development
	ISO/PWI TR 5255 (ISO, 2020)	ACS	Mobility integration low-speed automated driving architecture	Under development
	ISO7856 (ISO, 2022)	ACS	Remote support for low-speed automated driving	Under development
	ISO/TR 21186-3 (ISO, 2021i)	C-ITS	Security guidelines on the usage of standards	Under development
AUTOSAR	AUTOSAR 402 (AUTOSAR, 2009a)	In-vehicle Communication	Specification of crypto service manager	Published
	AUTOSAR 438 (AUTOSAR, 2009b)	In-vehicle Communication	Specification of crypto abstraction library	Published
	AUTOSAR 654 (AUTOSAR, 2017)	In-vehicle Communication	Specification of secure onboard communication	Published
	AUTOSAR 664 (AUTOSAR, 2015)	Vehicular Software	Overview of functional safety measures	Published
ETSI	ETSI TR 102 893 (ETSI, 2010a)	ITS	Threat, vulnerability and risk analysis	Published
	ETSI TS 102 731 (ETSI, 2010b)	ITS	Security services and architecture	Published
	ETSI TS 103 097 (ETSI, 2017)	ITS	Security header and certificate formats	Published
	ETSI TS 102 940 (ETSI, 2018)	ITS	Communications security architecture and management	Published
	ETSI TS 102 941 (ETSI, 2019)	ITS	Trust and privacy management	Published
	ETSI TS 102 942 (ETSI, 2012a)	ITS	Access control	Published
	ETSI TS 102 943 (ETSI, 2012b)	ITS	Confidentiality services	Published
	ETSI EN 302 637-2 (ETSI, 2014)	ITS	CAMs specifications	Published
PAS	PAS 1885:2018 (BSI, 2018b)	Vehicle Cybersecurity	The fundamental principles of automotive cyber security	Published
	PAS 11281:2018 (BSI, 2018a)	CAV	Impact of security on safety	Published
	PAS 1880 (BSI, 2020a)	CAV	Guidelines for developing and assessing control systems	Published
	PAS 1881 (BSI, 2020b)	CAV	Assuring the safety of automated vehicle trials	Published
W3C	Candidate (Gavigan et al., 2018)	Vehicle Cybersecurity	Vehicle information service specification	Under development
	Editor's Draft (Lee et al., 2021)	Vehicle Cybersecurity	Vehicle information access API	Under development
	WG Note (Reshetova and McCool, 2019)	IoT	Security and privacy guidelines	Under development

of CAVs and ACSs (ISO/TC204, 2019). Among the ISO/TC 204 efforts, ISO/TS 21177 (ISO, 2019c) was published to specify security and authenticity requirements for the exchanged data among OBUs, RSUs and TAs. The ISO/TS 21,177 will be replaced by ISO/CD 21,177 which is under development. The ISO 22737, which was published in July 2021, came up with the system requirements for the specific ACS case operating at level 4 of autonomy and with low-speed configuration (ISO, 2021c). ISO/AWI 21734 (ISO, 2021d) is a promising standard on which ISO/TC 204 is still progressing to present connectivity and safety requirements for the deploy-

ment of CAVs into public transportation through automated driving buses of all sizes. Moreover, and within the public transportation scope, the ISO 24014 (ISO, 2021a) was published in January 2021 and which highlights security management and identification schemes for all public transportation vehicles including the automated mini-buses. The ISO/TC 204 working groups are still developing further standards related to CAVs such as ISO/AWI TR 23254 (ISO, 2021f), which is about designing a high level referential architecture, and ISO/AWI TS 22726 (ISO, 2021g) for the vehicles' map database specifications. Further standards are still on early stages but they are dedicated to ACSs such as ISO/PWI TR 5255 (ISO, 2020) discussing low-speed automated driving system architecture and ISO7856 (ISO, 2022) presenting the specifications for ACSs remote assistance.

5.2. Automotive open system architecture (AUTOSAR)

Automotive industry has also pushed to standardise security approaches over on-board systems through their collaboration on AUTOSAR standards. AUTOSAR series tend for securing in-vehicle communication networks and ECUs, protecting data confidentially and implementing cryptography (Furst and Bechter, 2016) as detailed in Table 6. However, following AUTOSAR security specifications like AUTOSAR664 does not imply the vehicle compliance to ISO standards like ISO 26262 (AUTOSAR, 2015).

5.3. European telecommunication standards institute (ETSI)

Besides, ETSI is a European standard Organisation proposing many standards related to security and privacy on the ITS (ETSI, 2018). ETSI TC ITS WG5 working group focuses on identifying threats and their countermeasures, specifying requirements and building standardised architecture for CAVs communications (Lonc and Cincilla, 2016). Table 6 describes ETSI releases ensuring privacy preserving communication, exchanged certificates with RSUs, secured message formats, and PKI implementation.

5.4. European committee for standardization-European committee for electronical standardisation (CEN-CENELEC)

CEN founded CEN/TC 278 as the European ITS committee since 2013. Among its working groups, CEN/TC 278/WG16, which is fully joined with ISO TC 204 WG 18, has been focusing on V2I and V2V communications' standardisation (CEN/TC278, 2021a). The key published standard to cite within the context of security and data privacy is CEN ISO/TR 21186-3 (CEN/TC278, 2021b; ISO, 2021i) which provides guidelines on access control, and PKI for a secure automated driving ecosystem. Moreover, CEN/TC 278/WG17 focuses on urban ITS and has been developing new sets of standardisation initiatives dealing with the integration of CAVs to the urban infrastructure (CEN/TC278, 2018). The CEN/TC 278/WG17 publications represented first drafts of the ISO TC204/WG19 efforts once the two groups joined their contributions (Foss and Evensen, 2019).

Additionally, CEN and CENELEC consolidated their collaboration by creating CEN-CENELEC as a platform for the development of European standards through a wide range of sectors including transportation and information technologies (CEN-CENELEC, 2021). In collaboration with the European Commission, ISO, and other standardisation bodies, CEN-CENELEC created the CEN/CLC/JTC13 technical committee acting on cybersecurity and data protection field on a broad scope (CEN, 2021). As published on CEN-CENELEC program for 2021 (Cen-CENELEC, 2020), CEN/CLC/JTC13 aims to develop new cybersecurity standards for the IoT sector and privacy by design and by default within the context of the GDPR.

5.5. DATEX-II

Furthermore, transportation data exchange in Europe is controlled by DATEX II which is the road transport standard (Costantini et al., 2020). DATEX II was launched by CEN to address traffic data sharing and transmission including transmitted data in cooperative and connected mobility (DATEX-II, 2022b). Among its specifications, DATEX II 3.1 proposes a standardised message format between vehicles and RSUs which support the standardisation of V2I communication (DATEX-II, 2022a).

5.6. Publicly available specification (PAS)

BSI, the UK standardisation body, has developed a series of Publicly Available Specification (PAS) standards dedicated to CAVs cybersecurity related topics. PAS 1885:2018 (BSI, 2018b) represents a high level set of guidelines discussing the fundamental principles of cybersecurity over the development and use lifecycle. Additionally, PAS 11281:2018 came afterwards with more detailed recommendations for managing security risks impacting the safety (BSI, 2018a). Newer BSI standards such as PAS 1880 (BSI, 2020a) and PAS 1881 (BSI, 2020b) should be considered as they are acknowledging the consequences of cyber attacks over the vehicle safety.

5.7. World wide web consortium (W3C)

The W3C, specialised on developing web standards, has two working groups who published candidate standards, applicable to the vehicular environment, and which are intending to become standards according to W3C documentation classes W3C (2022). W3C has launched the Automotive Working Group who proposed on 2018 a recommendation on the Vehicle Information Service specification (Gavigan et al., 2018). The recommendation specifies how the in-vehicle system, that is responsible for exposing vehicle signals and data to on-board clients, communicates with other vehicles and devices via WebSocket. The recommendation advocates security access control mechanisms such as token and encryption using PKI. The Automotive Working Group has also published the Vehicle Information API Specification providing access restrictions to the vehicle data (Lee et al., 2021). The second working group is the WEB of Things working group who is focusing on standards enabling integration across IoT systems including IoV. In November 2019, the group disclosed a non-normative guidance of security and privacy using threat model describing the key security stakeholders, potential attackers and attack surfaces of IoT systems in a generic view (Reshetova and McCool, 2019).

5.8. Standards summary

Through an in-depth review of the core standardisation actors, this section presented a selection of key standards that are appropriate to cybersecurity and data privacy within the driverless environment. Additionally, since the initiation of the present work, a tracking of all new standards' related publications was conducted to provide up to date analysis and findings that keep pace with the rapidly evolving technologies of the ACS landscape.

Under the auspices of ISO standards, including their joint efforts to CEN-CENELEC, the ISO/TC22 and ISO/TC204 conceived a rich directory of standards for cybersecurity daunting challenges within ITS and smart cities. The recently published ISO/SAE 21,434 represents the most eagerly awaited standard covering cybersecurity guidelines for road vehicles. Though, the standard scope is broad enough to wrap all vehicles with electrical and electronic systems that can match any SAE automation level. Likewise, the ISO/SAE

21,434 scope covers only the in-vehicle component and not external systems through which potential attacks can occur. Hence, further standards need to be joined to the flamboyant ISO/SAE 21,434 for a more comprehensive security assessment. Even in their larval state, other standards remain constructive and more specific to ACSs such as ISO/AWI21734, ISO/PWI TR5255 and ISO7856. However, they are not directly addressing the cybersecurity risks.

Besides, AUTOSAR, ETSI and PAS published alluring guidelines on implementing security by design at different layers within a connected vehicular environment; still they need to be upgraded to tackle highly automated vehicles such as ACSs. Regarding data privacy concerns, DATEX-II is standardising the exchanged messages within the vehicular context, while W3C is working on more specific privacy guidelines within IoT settings. However, both efforts remain generic without approaching specific measures on protecting personal data within the ACS that has different data controllers.

As a matter of fact, the answer to our RQ4 is foreseen to be a partial and temporal "NO", as the existing standards need some leveraging, fusion and enhancement to build a comprehensive security framework which is intended to be our future work as discussed in Section 6.

6. Discussion & future work

With the intrinsic super smart in-vehicle components (hardware and software), its rich input and output data, and their communication with anything and everything, the ACS might not reach complete cyber safety without being built within a standardised framework and strong policies. However, some future work is still required and limitations should be noted. The present section depicts the required efforts from security, privacy and standardisation perspectives.

6.1. Future work related to security certification

Reaching a complete secure vehicular system seems to be impossible according to Linkov et al. (2019). Therefore, an effective strategy would not be eliminating them but being prepared for their occurrence and knowing how to adequately react to their impact. Consequently, as a future work, we are currently working on proposing a certification model using security- and privacy-by-design approaches to establish a thorough security audit. We elevate the results of the present work further by evaluating the existing standards, which thereafter are processed (selecting the best standards, propose improvements and make them more specific towards the CAV ecosystem) to constitute the skeleton of our proposed certification model. To this end, the certification model will tie together the organisational procedures, risk and threat assessment approaches and recommendations of the most adequate patching, scanning and penetration testing methods. Thereupon, our intended certification model would present the road map for security auditing of highly automated vehicles.

6.2. Future work related to data privacy

With regard to the privacy by design of ACS, there is a need to have more clarity on the various technical measures implemented at the ACS such as anonymisation and pseudonymisation. Still there is much debate about the effectiveness of the anonymisation technologies and the inherent risk to de-anonymize data by using reverse engineering technologies or by combining anonymized data with other information leading to identify a person. As a future work, we are progressing on identifying the compatibility of privacy laws with security technologies focusing on the gap between the legal definitions and the technological implementation of pseudonymisation and anonymisation.

6.3. Work limitations

Furthermore, the number of standards from various standardisation bodies at any stage, published or under development, changes very often which requires a recurrent update of the standards findings. Moreover, multiple standards can be overlapping, like ETSI standards that are partly rivalling with CEN and ISO sets; which let the concern open to the OEM or the service provider to select the standard to which they are seeking compliance. Finally, the cost to dive deeply into some standards represents a real limitation of the present review since the research was done based on the standard description or through free institutional resources.

7. Conclusion

With the advancements in the domain of CAVs, authorities are looking into integrating these, as ACSs, into the traditional public transports, either to extend or to replace existing services. The introduction of the ACS brings promise of great benefits to its citizens, especially for those with special needs, making public transport more personalised. However, as with everything Internet capable, it inherits its flaws and dangers in addition to being a 'new' vehicle that is still in its infancy. As the use of these mini-buses are intended to no longer have a driver (legally still required in many countries), it is up to the services provided to its users to ensure a comfortable and safe journey. This endeavour involves a significant amount of digital services and a complex infrastructure for operating a fleet of automated mini-buses, which require always to be connected and communicating in real-time.

Consequently, the goal of the present work is to provide a united and collated source of references for any researcher to look into when analysing associated cybersecurity and data privacy risks of integrating ACS in his/her city on the way to the future development. We want to have a holistic approach to include three facets of the risk plan (security, data protection, standards) in a singular framework for ACS integration into smart cities' operational environment.

In each facet, extensive analyses have been provided by pointing out the gaps and shortcomings in regard to this comprehensive view. A systematic categorisation and a mapping within each of the domains provides structuring and clarity on the scope of the threat landscape and efforts by the research community, the authorities and public & private organisations. Furthermore, based on a thorough investigation of the latest technologies and regulators efforts, the paper provides a novel and up to date reference of threats, technical and legal mitigation strategies to the ACS as a specific case of the IoV domain.

For cybersecurity, we defined two layers on which cyber attacks can occur, 'in-vehicle threats' dealing with the internals of the vehicle and 'communication threats' that includes all different types of possible communication that may influence the operation of a mini-bus. The attack surfaces have been further analysed and associated mitigation techniques have been aggregated into six mitigation strategies providing in-depth technical review relevant to ACS and their commonalities with CAV, ITS and IoV landscape. As the human factors in greatly to any effective defence strategy, cybersecurity regulations are essential to any ICT infrastructure. This work looked at the main key players from different governmental authorities EU, UK, USA, Japan as well as intergovernmental working groups. In regard to the data privacy, clarity is provided through identification of the laws, guidelines and recommendations from the different regulatory bodies (key players). Three major technical mitigation solutions were analysed concerning the safe storage and

transmission of data and are highlighting the importance of employing good data privacy solutions. The data privacy regulations have been summarised into the hard and soft laws, aggregating the most relevant regulations and laws from EU, international and intergovernmental initiatives, while underlining the new efforts being made towards CAVs. The last domain, summarised the main (seven) standardisation bodies and their standards regarding the cybersecurity and data privacy. It further provides insights in how these organisations operate, joined efforts and specialise in specific domains relevant to the ACS ecosystem.

This work brought together the key pieces of information on cybersecurity and data privacy relevant to the exploitation of ACSs. It can be summarised that great efforts are made in each of the domains and are expected to continue alongside the evolvement of the CAV, ITS and IoV in terms of technological progress, deployment environments (urban, suburban and rural requirements) and business-models & services (inter-transport connectivity, advertisement strategies, on-demand flexibility).

Declaration of Competing Interest

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

CRediT authorship contribution statement

Meriem Benyahya: Conceptualization, Methodology, Investigation, Visualization, Writing – original draft. **Anastasija Collen:** Writing – review & editing, Supervision. **Sotiria Kechagia:** Writing – review & editing. **Niels Alexander Nijdam:** Supervision, Visualization, Writing – review & editing.

Acknowledgments

This work has been funded and supported by the European Union's Horizon 2020 Research and Innovation Programme through AVENUE project (https://h2020-avenue.eu/) under grant agreement no. 769033, nIoVe project (https://www.niove.eu/) under grant agreement no. 833742 and SHOW project (https://show-project.eu/) under grant agreement no. 875530. The authors would also like to thank Allan Berrocal, from University of Costa Rica, for his insightful recommendations and orientations.

References

ACEA, 2020. ACEA Comments EDPB Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. Technical Report. ACEA.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., Ylianttila, M., 2019. Security for 5G and beyond. IEEE Commun. Surv. Tutor. 21 (4), 3682–3722. doi:10.1109/COMST.2019.2916180.

Ainsalu, J., Arffman, V., Bellone, M., Ellner, M., Haapamäki, T., Haavisto, N., Josefson, E., Ismailogullari, A., Lee, B., Madland, O., Madžulis, R., Müür, J., Mäkinen, S., Nousiainen, V., Pilli-Sihvola, E., Rutanen, E., Sahala, S., Schønfeldt, B., Smolnicki, P.M., Soe, R.M., Sääski, J., Szymańska, M., Vaskinn, I., Åman, M., 2018. State of the art of automated buses. Sustainability (Switzerland) 10 (9). doi:10.3390/su10093118.

Al Mamun, A., Abdullah Al Mamun, M., Shikfa, A., 2018. Challenges and mitigation of cyber threat in automated vehicle: an integrated approach. In: 2018 International Conference of Electrical and Electronic Technologies for Automotive, AUTOMOTIVE 2018, pp. 1–6. doi:10.23919/EETA.2018.8493171.

Ali, I., Li, F., 2020. An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs. Veh. Commun. 22, 100228. doi:10.1016/j.vehcom.2019.100228.

Ali Alheeti, K.M., Mc Donald-Maier, K., 2018. Intelligent intrusion detection in external communication systems for autonomous vehicles. Syst. Sci. Control Eng. 6 (1), 48–56. doi:10.1080/21642583.2018.1440260.

Almuhammadi, S., Neuman, C., 2005. Security and privacy using one-round zero-knowledge proofs. In: Proceedings - Seventh IEEE International Conference on E-Commerce Technology, CEC 2005, vol. 2005, pp. 435–438. doi:10.1109/ICECT.2005.78.

Article 29 Data Protection Working Party, 2017. Opinion 03/2017 on Processing Personal Data in the Context of Cooperative Intelligent Transport Systems (C-ITS) - 217/EN - WP 252. Technical Report. Article 29 Data Protection Working Party.

Asghar, M.N., Kanwal, N., Lee, B., Fleury, M., Herbst, M., Qiao, Y., 2019. Visual surveillance within the eu general data protection regulation: a technology perspective. IEEE Access 7, 111709–111726. doi:10.1109/ACCESS.2019.2934226.

Asuquo, P., Cruickshank, H., Morley, J., Ogah, C.P., Lei, A., Hathal, W., Bao, S., Sun, Z., 2018. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet Things J. 5 (6), 4778–4802. doi:10.1109/JIOT.2018.2820039.

Australia, N., 2018. Regulating Government Access to C-ITS and Automated Vehicle Data. Technical Report. National Transport Commission.

Auto-ISAC. Best Practices. https://automotiveisac.com/best-practices/.

AUTOSAR, 2009. Autosar 402 Specification of Crypto Service Manager. Technical Report. AUTOSAR.

AUTOSAR, 2009. Autosar 438 Specification of Crypto Abstraction Library. Technical Report. AUTOSAR.

AUTOSAR, 2015. Autosar 664 Overview of Functional Safety Measures in AUTOSAR. Technical Report. Autosar.

AUTOSAR, 2017. Autosar 654 Specification of Secure Onboard Communication. Technical Report. AUTOSAR.

Bailey, D., 2018. Quantitative Cybersecurity Risk Management for Autonomous Vehicle Systems. Technical University of Munich Ph.D. thesis. https://mediatum.ub.tum.de/doc/1482036/992686146856.pdf

Baqer, M., Krings, A., 2019. Reliability of VANET bicycle safety applications in malicious environments. In: 27th Telecommunications Forum, TELFOR 2019, pp. 2019–2022. doi:10.1109/TELFOR48224.2019.8971200.

Bezemskij, A., Loukas, G., Gan, D., Anthony, R.J., 2018. Detecting cyber-physical threats in an autonomous robotic vehicle using Bayesian networks. In: Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017, 2018-Janua, pp. 98–103. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.20.

Bhargava, B., Johnson, A.M., Munyengabe, G.I., Angin, P., 2016. A systematic approach for attack analysis and mitigation in V2V networks. J. Wirel. Mob. Netw., Ubiquitous Comput., Dependable Appl. 7 (1), 79–96. doi:10.22667/JOWUA.2016.03.31.079.

Bhusal, N., Gautam, M., Benidris, M., 2020. Cybersecurity of electric vehicle smart charging management systems. arXiv.

Bonichon, R., Canet, G., Correnson, L., Goubault, E., Haucourt, E., Hirschowitz, M., Labbé, S., Mimram, S., Flammini, F., Bologna, S., Vittorini, V., 2019. Computer Safety, Reliability, and Security, vol. 6894. Springer, Turku doi:10.1007/978-3-642-24270-0.

Bösch, P.M., Becker, F., Becker, H., Axhausen, K.W., 2018. Cost-based analysis of autonomous mobility services. Transp. Policy 64 (February), 76–91. doi:10.1016/j.tranpol.2017.09.005.

Boukerche, A., Siddiqui, A.J., Mammeri, A., 2017. Automated vehicle detection and classification: models, methods, and techniques. ACM Comput. Surv. 50 (5), 1–39. doi:10.1145/3107614.

BSI, 2018. PAS 11281 Connected and Autonomous Vehicles (CAVs). Technical Report. BSI.

BSI, 2018. PAS 1885:2018 How to Improve and Maintain Vehicle Security. Technical Report. BSI.

BSI, 2020. PAS 1880 Guidelines for Developing and Assessing Control Systems for Automated Vehicles. Technical Report. BSI.

BSI, 2020. PAS 1881: Assuring the Safety of Automated Vehicle Trials and Testing-Specifi Cation Publishing and Copyright Information. Technical Report. BSI.

C-Roads, 2021. Platform: C-Roads. https://www.c-roads.eu/platform.html.

Cao, Y., Zhou, Y., Chen, Q. A., Xiao, C., Park, W., Fu, K., Cyr, B., Rampazzi, S., Morley Mao, Z., 2019. Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving. arXiv, 2267–2281.

Casola, V., De Benedictis, A., Rak, M., Villano, U., 2018. Towards automated penetration testing for cloud applications. In: Proceedings - 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE 2018. Institute of Electrical and Electronics Engineers Inc., pp. 30–35. doi:10.1109/WETICE.2018.00012.

CEN, 2021. CEN/CLC/JTC 13 - Cybersecurity and Data Protection. https://standards.cen.eu/.

Cen-CENELEC, 2020. Work Programme 2021. Technical Report. CEN-CENELEC.

CEN-CENELEC, 2021. About us - CEN-CENELEC. https://www.cencenelec.eu/aboutus/Pages/default.aspx.

CEN/TC278, 2018. European Standardization in Support of urban Intelligent Transportation and Mobility. Technical Report. CEN. https://www.cen.eu/news/brochures/brochures/Urban_Intelligent_Transport_CEN-TC-278.pdf

CEN/TC278, 2021a. CEN/TC 278 Intelligent transport systems. https://www.itsstandards.eu/aboutus/.

CEN/TC278, 2021. Cooperative Intelligent Transport Systems (C-ITS) Guidelines on the Usage of Standards. Technical Report. CEN and ISO.

Changalvala, R., Malik, H., 2019. LiDAR data integrity verification for autonomous vehicle. IEEE Access 7, 138018–138031. doi:10.1109/ACCESS.2019.2943207.

Cho, K.T., Shin, K.G., 2016. Error handling of in-vehicle networks makes them vulnerable. In: Proceedings of the ACM Conference on Computer and Communications Security, 24-28-Octo, pp. 1044–1055. doi:10.1145/2976749.2978302.

Chowdhury, M., Islam, M., Khan, Z., 2019. Security of connected and automated vehicles. Bridge 49 (3), 46–56.

Chu, G., Lisitsa, A., 2019. Penetration testing for internet of things and its automa-

tion. In: Proceedings - 20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018. Institute of Electrical and Electronics Engineers Inc., pp. 1479–1484. doi:10.1109/HPCC/SmartCity/DSS.2018.00244.

Collard, G., Ducroquet, S., Disson, E., Talens, G., 2017. A definition of information security classification in cybersecurity context. In: Proceedings - International Conference on Research Challenges in Information Science. IEEE, pp. 77–82. doi:10.1109/RCIS.2017.7956520.

Collingwood, L., 2017. Privacy implications and liability issues of autonomous vehicles. Inf. Commun. Technol. Law 26 (1), 32–45. doi:10.1080/13600834.2017.1269871.

Congress, 2017. H3388- Self Drive Act. Technical Report. US Government. https://www.congress.gov/bill/115th-congress/house-bill/3388/text

Congress, 2019. S.2181 Spy Car Act. Technical Report. US Government. https://www.congress.gov/bill/116th-congress/senate-bill/2182/text

Cormode, G., 2011. Personal privacy vs. population privacy: learning to attack anonymization. In: Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1253–1261. doi:10.1145/2020408.2020598.

Costantini, F., Thomopoulos, N., Steibel, F., Curl, A., Lugano, G., Kováčiková, T., 2020. Autonomous vehicles in a GDPR era: an international comparison. Adv. Transp. Policy Plann. 5. doi:10.1016/bs.atpp.2020.02.005.

Crane, D.A., Logue, K.D., Pilz, B.C., 2017. A survey of legal issues arising from the deployment of autonomous and connected vehicles. SSRN Electron. J. 23 (2). doi:10.2139/ssrn.2807059.

Cui, J., Liew, L.S., Sabaliauskaite, G., Zhou, F., 2019. A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Netw. 90. doi:10.1016/j.adhoc.2018.12.006.

Daimi, K., Saed, M., 2018. Securing tire pressure monitoring system. In: The Fourteenth Advanced International Conference on Telecommunications, Barcelona, Spain, pp. 32–37.

Daniel J. Fagnant, Kockelman, K., 2015. Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transp. Res. Part A 77, 167–181.

Dasgupta, S., Rahman, M., Islam, M., Chowdhury, M., 2021. Prediction-based GNSS spoofing attack detection for autonomous vehicles. (arXiv:2010.11722v1 [cs.RO]). (arXiv Computer Science (864), 1–16.

Data for Road Safety, 2021. Partners Safety Related Traffic Information Ecosystem. https://www.dataforroadsafety.eu/.

DATEX-II, a. Datex II developments. https://datex2.eu/datex2/developments.

DATEX-II, b. Datex II Specifications. https://datex2.eu/datex2/specifications.

Department for Transport, 2015. The Pathway to Driverless Cars. Technical Report. Department of Transport, UK.

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., Yu, S., 2020. Attacks and defences on intelligent connected vehicles: a survey. Digit. Commun. Netw. 6 (4), 399–421. doi:10.1016/j.dcan.2020.04.007.

Duong-Ngoc, P., Tan, T.N., Lee, H., 2020. Efficient NewHope cryptography based facial security system on a GPU. IEEE Access 8, 108158–108168. doi:10.1109/ACCESS.2020.3000316.

Dwork, C., Roth, A., 2013. The algorithmic foundations of differential privacy. Found. Trends Theor. Comput. Sci. 9 (3–4), 211–487. doi:10.1561/0400000042.

El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P., 2020. Cybersecurity challenges in vehicular communications. Veh. Commun. 23, 100214. doi:10.1016/j.vehcom.2019.100214.

Elliott, D., Keen, W., Miao, L., 2019. Recent advances in connected and automated vehicles. J. Traffic Transp. Eng. (English Edition) 6 (2), 109–131. doi:10.1016/j.jtte.2018.09.005.

Ernst, J.M., Michaels, A.J., 2018. LIN bus security analysis. In: Proceedings: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, pp. 2085–2090. doi:10.1109/IECON.2018.8592744.

ETSI, 2010. ETSI TR 102 893 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). Technical Report. ETSI.

ETSI, 2010. TS 102 731 - V1.1.1 - Intelligent Transport Systems (ITS); Security; Security Services and Architecture. Technical Report. ETSI.

ETSI, 2012. TS 102 942 - V1.1.1 Intelligent Transport Systems (ITS); Security; Access Control Technical Specification. Technical Report. ETSI. http://portal.etsi.org/chaircor/ETSI_support.asp

ETSI, 2012. TS 102 943 V1.1.1 Intelligent Transport Systems (ITS); Security; Confidentiality services Technical Specification. Technical Report. ETSI.

ETSI, 2014. EN 302 637-2 - V1.3.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service. Technical Report. ETSI. https://www.etsi.org/deliver/etsi_en/302600_302699/30263702/01.03.01_30/en_30263702v010301v.pdf

ETSI, 2017. TS 103 097 - V1.3.1 - Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats. Technical Report. ETSI. https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

ETSI, 2018. ETSI TS 102 940 V1.3.1 - Security; ITS Communications Security Architecture and Security Management. Technical Report. ETSI. https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf

ETSI, 2019. TS 102 941 - V1.3.1 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. Technical Report. ETSI. https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf

European Automotive Manufacturers Association (ACEA), 2017. ACEA Principles of Automobile Cybersecurity. Technical Report. ACEA.

European Automotive Manufacturers Association (ACEA), 2019. Roadmap for the Deployment of Automated Driving in the European Union. Technical Report. ACEA.

European Commission, 2018. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). Technical Report. European Commission.

European Commissopn,. Cooperative, connected and automated mobility (CCAM) Mobility and Transport. https://ec.europa.eu/transport/themes/its/c-its.

European Data Protection Board, 2019. Opinion of EDPB on Interplay Between ePrivacy Directive and GDPR. Technical Report. EDPB. https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

European Data Protection Board, 2020. Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. Technical Report. EDPB.

European data Protection Board, 2021. Guidelines 1/2020 on Processing Personal Data in the Context of Connected Vehicles and Mobility Related Applications. Technical Report. EDPB. https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf

European Parliament and the Council of the European Union, 2002. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications). Technical Report. European Parliament and the Council of the European Union.

European Union Agency for Network and Information Security (ENISA), 2015. Cyber Security for Smart Cities. Technical Report. ENISA.

European Union Agency for Network and Information Security (ENISA), 2017. Cyber Security and Resilience of Smart Cars. Good Practices and Recommendations. Technical Report. ENISA.

European Union Agency for Network and Information Security (ENISA), 2019. ENISA Good Practices for the Security of Smart Cars. Technical Report. ENISA.

European Union Agency for Network and Information Security (ENISA), 2020. Cybersecurity Stocktaking in the CAM Stakeholder Mapping and Stocktaking of Connected. Technical Report. ENISA doi:10.2824/24902.

European Union Agency for Network and Information Security (ENISA), 2020. Guidelines for Securing the Secure supply chain for IoT. Technical Report. ENISA.

European Union Agency for Network and Information Security (ENISA), 2021. Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving. Technical Report. ENISA and JRC.

Fabian Biegel, A., Bongers, A., Feld, T., Jochem Berthold Maier, M., Marsch, C., Marti, A.P., Plass, C., Reinhardt, R., Schmieg German, A., Stark, J., Steinbuss, S., Strnadl, C.F., Weiss Christian Weiss, A., Wessel Sabine Wilfling, S., 2020. GAIA-X: Driver of Digital Innovation in Europe. Technical Report. GAIA-X.

Federal Ministry for Economic Affairs and Energy, 2020. GAIA-X: The European Project Kicks off the Next Phase. Technical Report. GAIA-X.

Ferrara, P., Mandal, A.K., Cortesi, A., Spoto, F., 2021. Static analysis for discovering IoT vulnerabilities. Int. J. Softw. Tools Technol. Trans. 23 (1), 71–88. doi:10.1007/s10009-020-00592-x.

Foss, T., Evensen, K., 2019. ITS Standardisering. Technical Report. Statens vegsen. https://its-norway.no/wp-content/uploads/2021/01/ITS-standardisering-SVV-rapport-482-4MB.pdf

Furst, S., Bechter, M., 2016. AUTOSAR for connected and autonomous vehicles: the AUTOSAR adaptive platform. In: Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN-W 2016, pp. 215–217. doi:10.1109/DSN-W.2016.24.

GAIA-X,. GAIA-X: A Federated Data Infrastructure for Europe. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

Gavigan, K., Crofts, A., Lee, W., Kinney, P., 2018. Vehicle Information Service Specification. Technical Report. W3C. https://www.w3.org/TR/2018/CR-vehicle-information-service-20180213/#introduction

Glancy, D.J., 2012. Privacy in autonomous vehicles. Number 4 Article 52 (4), 12–14.

GRVA UNECE, 2020. Proposal for the Interpretation Document for UN Regulation No. [155] on Uniform Provisions Concerning the Approval of Vehicles with Regards to Cyber Security and Cyber Security Management System. Technical Report. UNECE. https://unece.org/fileadmin/DAM/trans/doc/2020/wp29/WP29-182-05e.pdf

Gu, P., Khatoun, R., Begriche, Y., Serhrouchni, A., 2017. Vehicle driving pattern based sybil attack detection. In: Proceedings - 18th IEEE International Conference on High Performance Computing and Communications, 14th IEEE International Conference on Smart City and 2nd IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2016, pp. 1282–1288. doi:10.1109/HPCC-SmartCity-DSS.2016.0182.

Gupta, R., Tanwar, S., Kumar, N., Tyagi, S., 2020. Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: a systematic review. Comput. Electr. Eng. 86. doi:10.1016/j.compeleceng.2020.106717.

He, D., Zeadally, S., Xu, B., Huang, X., 2015. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. 10 (12), 2681–2691. doi:10.1109/TIFS.2015.2473820.

HM Government, 2017. The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles. Technical Report. Department of Transport, UK.

ICDPPC, 2017. Resolution on Data Protection in Automated and Connected Vehicles The 38th International Conference of Data Protection and Privacy Commissioners. Technical Report. ICDPPC.

Iclodean, C., Cordos, N., Varga, B.O., 2020. Autonomous shuttle bus for public transportation: areview. Energies 13 (11). doi:10.3390/en13112917.

Ioulianou, P.P., Vassilakis, V.G., Moscholios, I.D., Logothetis, M.D., 2018. A signature

based intrusion detection system for the internet of things. Information and Communication Technology Form.
ISO,. ISO/IEC 15408. https://www.iso.org/standard/50341.html.
ISO, 2014. ISO/IEC 1845:2008. Technical Report. ISO/IEC. https://www.iso.org/fr/standard/46412.html
ISO, 2015. ISO 9001:2015. https://www.iso.org/standard/62085.html.
ISO, 2018. International Standard ISO / IEC Information Technology – Security Techniques – Information Security Management Systems — Overview and. Technical Report. ISO/IEC. https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip
ISO, 2018b. ISO 20077-2:2018. https://www.iso.org/standard/67597.html.
ISO, 2018c. ISO 26262-1:2018. https://www.iso.org/standard/68383.html.
ISO, 2018. ISO/IEC20243. Technical Report. ISO/IEC.
ISO, 2019a. ISO 20078-3:2019. https://www.iso.org/standard/67579.html.
ISO, 2019b. ISO/PAS 21448:2019. https://www.iso.org/standard/70939.html.
ISO, 2019c. ISO/TS 21177:2019. https://www.iso.org/standard/70056.html.
ISO, 2020. ISO/PWI TR 5255-2. https://genorma.com/en/project/show/iso:proj:81070.
ISO, 2021a. ISO - ISO 24014-1:2021 - Public Transport – Interoperable Fare Management System – Part 1: Architecture. https://www.iso.org/standard/72507.html.
ISO, 2021b. ISO - ISO/DPAS 5112 - Road Vehicles – Guidelines for Auditing Cybersecurity Engineering. https://www.iso.org/standard/80840.html.
ISO, 2021. ISO 22737:2021. Technical Report. ISO. https://www.iso.org/standard/73767.html
ISO, 2021d. ISO/AWI 21734. https://www.iso.org/standard/71520.html.
ISO, 2021e. ISO/AWI 24089. https://www.iso.org/standard/77796.html.
ISO, 2021f. ISO/AWI TR 23254. https://www.iso.org/standard/75089.html.
ISO, 2021. ISO/AWI TS 22726. Technical Report. ISO. https://www.iso.org/standard/73747.html
ISO, 2021h. ISO/SAE DIS 21434. https://www.iso.org/standard/70918.html.
ISO, 2021. ISO/TR 21186. Technical Report. CEN and ISO. https://www.iso.org/standard/79949.html
ISO, 2022. ISO/NP 7856. https://genorma.com/en/project/show/iso:proj:82951.
ISO/TC204, 2019. ITS Standardization Activities of ISOTC 204. Technical Report. ISO.
ISO/TC22, 2021. ISO - ISO/SAE PAS 22736:2021 - Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. https://www.iso.org/standard/73766.html.
ITU-T, 2017. X.1373 Secure Software Update Capability for Intelligent Transportation System Communication Devices. Technical Report. ITU-T.
ITU-T, 2020. X. 1371 Security Threats to Connected Vehicles. Technical Report. ITU-T.
ITU-T, 2020. X.1372 Security Guidelines for Vehicle-to-Everything (V2X) Communication. Technical Report. ITU-T.
ITU-T, 2020. X.1374 Security Requirements for External Interfaces and devices with Vehicle Access Capability. Technical Report. ITU-T.
ITU-T, 2020. X.1375 Guidelines for an Intrusion Detection System for in-Vehicle Networks. Technical Report. ITU-T.
ITU-T, 2021a. ITU-T Recommendations. https://www.itu.int/ITU-T/recommendations/.
ITU-T, 2021. X.1376 Security-Related Misbehaviour Detection Mechanism Using Big Data for Connected Vehicles. Technical Report. ITU-T.
IWGDPT, 2018. International Working Group on Data Protection in Telecommunications. Technical Report. IWGDPT. https://fpf.org/wp-content/uploads/
J-Auto-ISAC,. J-Auto-ISAC for the safety and security of the automobile society. https://j-auto-isac.or.jp/.
JasPar, 2021. JasPar. https://www.jaspar.jp/en.
Jeon, J., Park, J.H., Jeong, Y.S., 2020. Dynamic analysis for IoT malware detection with convolution neural network model. IEEE Access 8, 96899–96911. doi:10.1109/ACCESS.2020.2995887.
Johari, R., Kaur, I., Tripathi, R., Gupta, K., 2020. Penetration testing in IoT network. In: Proceedings of the 2020 International Conference on Computing, Communication and Security, ICCCS 2020. Institute of Electrical and Electronics Engineers Inc. doi:10.1109/ICCCS49678.2020.9276853.
Joy, J., Gerla, M., 2017. Privacy risks in vehicle grids and autonomous cars. In: CarSys 2017 - Proceedings of the 2nd ACM International Workshop on Smart, Autonomous, and Connected Vehicular Systems and Services, Co-Located with MobiCom 2017, pp. 19–23. doi:10.1145/3131944.3133938.
Kang, J., Yu, R., Huang, X., Jonsson, M., Bogucka, H., Gjessing, S., Zhang, Y., 2016. Location privacy attacks and defenses in cloud-enabled internet of vehicles. IEEE Wirel. Commun. 23 (5), 52–59. doi:10.1109/MWC.2016.7721742.
Kang, M.J., Kang, J.W., 2016. Intrusion detection system using deep neural network for in-vehicle network security. PLoS One 11 (6), 1–17. doi:10.1371/journal.pone.0155781.
Karati, A., Hafizul Islam, S.K., Biswas, G.P., Bhuiyan, M.Z.A., Vijayakumar, P., Karuppiah, M., 2018. Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments. IEEE Internet Things J. 5 (4), 2904–2914. doi:10.1109/JIOT.2017.2741580.
Karnouskos, S., Kerschbaum, F., 2018. Privacy and integrity considerations in hyperconnected autonomous vehicles. Proc. IEEE 106 (1), 160–170. doi:10.1109/JPROC.2017.2725339.
Kawamoto, Y., Murakami, T., 2018. On the anonymization of differentially private location obfuscation; on the anonymization of differentially private location obfuscation. 2018 International Symposium on Information Theory and Its Applications (ISITA).
Kawanishi, Y., Nishihara, H., Souma, D., Yoshida, H., Hata, Y., Schoitsch, E., 2019. A comparative study of JASO TP15002-based security risk assessment methods for connected vehicle system design. Secur. Commun. Netw. 2019 (vi). doi:10.1155/2019/4614721.
Khan, S.K., Shiwakoti, N., Stasinopoulos, P., Chen, Y., 2020. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. Accid. Anal. Prev. 148 (October), 105837. doi:10.1016/j.aap.2020.105837.
Khanam, S., Ahmedy, I.B., Idna Idris, M.Y., Jaward, M.H., Bin Md Sabri, A.Q., 2020. A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things. IEEE Access 8, 219709–219743. doi:10.1109/ACCESS.2020.3037359.
Kim, K., Kim, J.S., Jeong, S., Park, J.H., Kim, H.K., 2021. Cybersecurity for autonomous vehicles: review of attacks and defense. Comput. Secur. 103, 102150. doi:10.1016/j.cose.2020.102150.
Kim, S., Kim, R.Y.C., Park, Y.B., 2016. Software vulnerability detection methodology combined with static and dynamic analysis. Wirel. Personal Commun. 89 (3), 777–793. doi:10.1007/s11277-015-3152-1.
Klinedinst, D., King, C., 2016. On board diagnostics: risks and vulnerabilities of the connected vehicle. CERT Coordination Center, SEI Tech. Rev. 21. https://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf
Kobayashi, H., Konno, C., Kayashima, M., Nakano, M., 2013. Approaches for Vehicle Information Security. Technical Report. IPA. https://www.ipa.go.jp/files/000033402.pdf
KPMG, 2020. Assessing the Preparedness of 30 Countries and Jurisdictions in the Race for Autonomous Vehicles 2020 Autonomous Vehicles Readi Ness I Ndex. Technical Report. KPMG.
Krontiris, I., Grammenou, K., Terzidou, K., Zacharopoulou, M., Tsikintikou, M., Baladima, F., Sakellari, C., Kaouras, K., 2020. Autonomous vehicles: data protection and ethical considerations. In: Proceedings - CSCS 2020: ACM Computer Science in Cars Symposium doi:10.1145/3385958.3430481.
Lee, M., Atkison, T., 2020. VANET applications: past, present, and future. Veh. Commun. 1, 100310. doi:10.1016/j.vehcom.2020.100310.
Lee, W., An, Q., Crofts, A., Gavigan, K., Park, J., Rees, K., 2021. Vehicle Information Access API. Technical Report. W3C. https://rawgit.com/w3c/automotive/master/vehicle_data/vehicle_spec.html
Li, C., Fu, Y., Yu, F.R., Luan, T.H., Zhang, Y., 2020. Vehicle position correction: a vehicular blockchain networks-based GPS error sharing framework. IEEE Trans. Intell. Transp. Syst. PP, 1–15. doi:10.1109/tits.2019.2961400.
Li, Z., Zou, D., Tang, J., Zhang, Z., Sun, M., Jin, H., 2019. A comparative study of deep learning-based vulnerability detection system. IEEE Access 7, 103184–103197. doi:10.1109/ACCESS.2019.2930578.
Lim, H.S.M., Taeihagh, A., 2018. Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications. Energies 11 (5), 1062. doi:10.3390/en11051062.
Lim, J., Yu, H., Kim, K., Kim, M., Lee, S.B., 2017. Preserving location privacy of connected vehicles with highly accurate location updates. IEEE Commun. Lett. 21 (3), 540–543. doi:10.1109/LCOMM.2016.2637902.
Lin, B.-R., Kifer, D., 2014. Towards a systematic analysis of privacy definitions. J. Privacy Confid. 5 (2), 57–109. doi:10.29012/jpc.v5i2.631.
Lin, K.L., Shih, C.S.D., Li, J.R., 2019. From rail to railless: retrofitting servicing buses for safe autonomous public transportation. In: 2019 IEEE International Conference on Embedded Software and Systems, ICESS 2019, pp. 1–8. doi:10.1109/ICESS.2019.8782530.
Linkov, V., Zámecník, P., Havlícková, D., Pai, C.W., 2019. Human factors in the cybersecurity of autonomous vehicles: trends in current research. Front. Psychol. 10 (MAY), 1–7. doi:10.3389/fpsyg.2019.00995.
Liu, S., Kong, L., Wang, H., 2018. Face detection and encryption for privacy preserving in surveillance video. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11258 LNCS, pp. 162–172. doi:10.1007/978-3-030-03338-5_14.
Lonc, B., Cincilla, P., 2016. Cooperative ITS security framework: standards and implementations progress in Europe. WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks doi:10.1109/WoWMoM.2016.7523576.
Lozano, M., Sanguino, M., 2019. Review on V2X, I2X, and P2X communications and their applications: a comprehensive analysis over time. Sensors 1–29. Figure 1
Lu, Z., Qu, G., Liu, Z., 2019. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Trans. Intell. Transp. Syst. 20 (2), 760–776. doi:10.1109/TITS.2018.2818888.
Macher, G., Schmittner, C., Veledar, O., Brenner, E., 2020. ISO/SAE DIS 21434 automotive cybersecurity standard - in a nutshell. In: Computer Safety, Reliability, and Security. Springer, Cham, pp. 123–135. doi:10.1007/978-3-030-55583-2_9.
Manivannan, D., Moni, S.S., Zeadally, S., 2020. Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs). Veh. Commun. 25, 100247. doi:10.1016/j.vehcom.2020.100247.
Maple, C., Bradbury, M., Le, A.T., Ghirardello, K., 2019. A connected and autonomous vehicle reference architecture for attack surface analysis. Appl. Sci. (Switzerland) 9 (23). doi:10.3390/app9235101.
Marksteiner, S., Ma, Z., 2019. Approaching the automation of cyber security testing of connected vehicles. In: ACM International Conference Proceeding Series, pp. 4–6. doi:10.1145/3360664.3360729.
Mazloom, S., Rezaeirad, M., Hunter, A., McCoy, D., 2016. A security analysis of an in vehicle infotainment and app platform. 10th USENIX Workshop on Offensive Technologies, WOOT 2016.
METI, 2018. Cyber Security Measures in Automated Driving Systems. Technical Report. Ministry of Economy, Trade and Industry.
Meyer, J., Becker, H., Bösch, P.M., Axhausen, K.W., 2017. Autonomous vehicles: the next jump in accessibilities? Res. Transp. Econ. 62, 80–91. doi:10.1016/j.retrec.2017.03.005.

Miller, C., Valasek, C., 2015. Remote exploitation of an unaltered passenger vehicle. Defcon 23 2015, 1–91.
Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H., Baik, S.W., 2018. Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans. Ind. Inf. 14 (8), 3679–3689. doi:10.1109/TII.2018.2791944.
Murati, E., Hënkoja, M., 2019. Location data privacy on MaaS under GDPR. Eur. J. Privacy L. & Tech. 115. http://arxiv.org/abs/1607.02177
Mushtaq, M.F., Jamel, S., Disina, H., Pindar, Z.A., Shafinaz, N., Shakir, A., Deris, M.M., 2017. A survey on the cryptographic encryption algorithms. IJACSA International Journal of Advanced Computer Science and Applications 8 (11), 333–344. doi:10.14569/IJACSA.2017.081141.
National Science and Technology Council and the United States Department of Transportation, 2020. Ensuring American Leadership in Automated Vehicle Technologies, Automated Vehicles 4.0. Technical Report. US Government. https://www.transportation.gov/av/4
Nayak, T.K., Adeshiyan, S.A., Zhang, C., 2016. A concise theory of randomized response techniques for privacy and confidentiality protection. Handb. Stat. 34 (December), 273–286. doi:10.1016/bs.host.2016.01.015.
Nguyen, H.N., Tavakoli, S., Shaikh, S.A., Maynard, O., 2019. Developing a QRNG ECU for automotive security: experience of testing in the real-world. In: Proceedings - 2019 IEEE 12th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2019. Institute of Electrical and Electronics Engineers Inc., pp. 61–68. doi:10.1109/ICSTW.2019.00033.
Nguyen, K.T., Laurent, M., Oualha, N., 2015. Survey on secure communication protocols for the internet of things. Ad Hoc Netw. 32, 17–31. doi:10.1016/j.adhoc.2015.01.006.
NHTSA, 2017. Automated Driving Systems A vision for Safety. Technical Report. NHTSA.
NHTSA, 2021. Vehicle Cybersecurity. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.
Noh, J., Jeon, S., Cho, S., 2020. Distributed blockchain-based message authentication scheme for connected vehicles. Electronics (Switzerland) 9 (1). doi:10.3390/electronics9010074.
Oham, C., Michelin, R.A., Jurdak, R., Kanhere, S.S., Jha, S., 2021. B-FERL: blockchain based framework for securing smart vehicles. Inf. Process. Manag. 58 (1), 102426. doi:10.1016/j.ipm.2020.102426. https://doi.org/10.1016/j.ipm.2020.102426
Oxford English Dictionary, 2021. Home : Oxford English Dictionary. https://www.oed.com/.
Pan, L., Zheng, X., Chen, H.X., Luan, T., Bootwala, H., Batten, L., 2017. Cyber security attacks to modern vehicular systems. J. Inf. Secur. Appl. 36, 90–100. doi:10.1016/j.jisa.2017.08.005.
Parkinson, S., Ward, P., Wilson, K., Miller, J., 2017. Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. 18 (11), 2898–2915. doi:10.1109/TITS.2017.2665968.
Pattinson, J.A., Chen, H., Basu, S., 2020. Legal issues in automated vehicles: critically considering the potential role of consent and interactive digital interfaces. Humanit. Social Sci. Commun. 7 (1). doi:10.1057/s41599-020-00644-2.
Personal Information Protection Commission, 2016. Amended Act on the Protection of Personal Information. Technical Report. PPC. https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf
Pesé, M.D., Schmidt, K., Zweck, H., 2017. Hardware/software co-design of an automotive embedded firewall. SAE Technical Papers. SAE International doi:10.4271/2017-01-1659.
Petit, J., Shladover, S.E., 2015. Potential cyberattacks on automated vehicles. IEEE Trans. Intell. Transp. Syst. 16 (2), 546–556. doi:10.1109/TITS.2014.2342271.
Petit, J., Stottelaar, B., Feiri, M., Kargl, F., 2015. Remote attacks on automated vehicles sensors: experiments on camera and LiDAR. Blackhat.com 1–13.
Ren, K., Wang, Q., Wang, C., Qin, Z., Lin, X., 2020. The security of autonomous driving: threats, defenses, and future directions. Proc. IEEE 108 (2), 357–372. doi:10.1109/JPROC.2019.2948775.
Reshetova, E., McCool, M., 2019. Web of Things (WoT) Security and Privacy Guidelines. Technical Report. W3C. https://www.w3.org/TR/2019/NOTE-wot-security-20191106/
Russell, R., Kim, L., Hamilton, L., Lazovich, T., Harer, J., Ozdemir, O., Ellingwood, P., McConley, M., 2019. Automated vulnerability detection in source code using deep representation learning. In: Proceedings - 17th IEEE International Conference on Machine Learning and Applications, ICMLA 2018, pp. 757–762. doi:10.1109/ICMLA.2018.00120.
SAE, 2018. J3016B Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles. Technical Report. SAE.
Sarker, A., Shen, H., Rahman, M., Chowdhury, M., Dey, K., Li, F., Wang, Y., Narman, H.S., 2020. A review of sensing and communication, human factors, and controller aspects for information-aware connected and automated vehicles. IEEE Trans. Intell. Transp. Syst. 21 (1), 7–29. doi:10.1109/TITS.2019.2892399.
Schmittner, C., Dobaj, J., MacHer, G., Brenner, E., 2020. A preliminary view on automotive cyber security management systems. In: Proceedings of the 2020 Design, Automation and Test in Europe Conference and Exhibition, DATE 2020. Institute of Electrical and Electronics Engineers Inc., pp. 1634–1639. doi:10.23919/DATE48585.2020.9116406.
Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P., 2016. Using SAE J3061 for automotive security requirement engineering. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9923 LNCS, pp. 157–170. doi:10.1007/978-3-319-45480-1_13.
Schmittner, C., Macher, G., 2019. Automotive cybersecurity standards - relation and overview. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 11699 LNCS, pp. 153–165. doi:10.1007/978-3-030-26250-1_12.
Schoitsch, E., Schmittner, C., 2020. Ongoing cybersecurity and safety standardization activities related to highly automated/autonomous vehicles. In: Intelligent System Solutions for Auto Mobility and Beyond. Springer, Cham, pp. 72–86. doi:10.1007/978-3-030-65871-7_6.
Sheehan, B., Murphy, F., Mullins, M., Ryan, C., 2019. Connected and autonomous vehicles: a cyber-risk classification framework. Transp. Res. Part A 124, 523–536. doi:10.1016/j.tra.2018.06.033.
Shin, H., Kim, D., Kwon, Y., Kim, Y., 2017. Illusion and dazzle: adversarial optical channel exploits against lidars for automotive applications. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10529 LNCS, pp. 445–467. doi:10.1007/978-3-319-66787-4_22.
Śmieszek, M., Dobrzańska, M., 2015. Application of Kalman filter in navigation process of automated guided vehicles. Metrol. Meas. Syst. 22 (3), 443–454. doi:10.1515/mms-2015-0037.
Smith, G., Smith, G., 2020. Making Mobility-as-a-Service. Chalmers University of Technology, Gothenburg.
Suh, S.-B., 2020. Understanding the UNECE WP.29 Cybersecurity Regulation | PERSEUS. https://cyberperseus.com/understanding-the-unece-wp-29-cybersecurity-regulation/.
Suo, D., Moore, J., Boesch, M., Post, K., Sarma, S.E., 2020. Location-based schemes for mitigating cyber threats on connected and automated vehicles: a survey and design framework. IEEE Trans. Intell. Transp. Syst. 1–19. doi:10.1109/TITS.2020.3038755.
Taeihagh, A., Lim, H. S. M., 2018. Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. arXiv.
Takahashi, J., Aragane, Y., Miyazawa, T., Fuji, H., Yamashita, H., Hayakawa, K., Ukai, S., Hayakawa, H., 2017. Automotive attacks and countermeasures on LIN-Bus. J. Inf. Process. 25 (3), 220–228. doi:10.2197/ipsjjip.25.220.
Takbiri, N., Houmansadr, A., Goeckel, D.L., Pishro-Nik, H., 2017. Limits of location privacy under anonymization and obfuscation. In: IEEE International Symposium on Information Theory - Proceedings, pp. 764–768. doi:10.1109/ISIT.2017.8006631.
Tashiro, A., Muraoka, H., Araki, S., Kakizaki, K., Uehara, S., 2018. A secure protocol consisting of two different security-level message authentications over CAN. In: 2017 3rd IEEE International Conference on Computer and Communications, ICCC 2017, 2018-Janua, pp. 1520–1524. doi:10.1109/CompComm.2017.8322794.
The Data Protection WG of the C-ITS Platform, 2016. C-ITS Platform Final Report. Technical Report. C-ITS Platform.
The European Parliament and of the Council, 2019. Regulation (EU) 2019/2144. Technical Report. European Union.
The European Parliament and the Council of the European Union, 2016. Directive (EU) 2016/ 1148 of the European Parliament and of the Council - NIS Dircetive 1. Technical Report. European Commission.
The European Parliament and the Council of the European Union, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Technical Report. European Commission.
The European Parliament and the Council of the European Union, 2020. Proposal for a Directive Directive (EU) 2016/ 1148 of the European Parliament and of the Council - NIS Dircetive 2. Technical Report. European Commission, Brussels.
The UK Centre for Connected and Autonomous Vehicles, 2020. Innovation is Great: Connected and Automated vehicles. Technical Report. Department of Transport, UK.
Toledo, J., Piñeiro, J.D., Arnay, R., Acosta, D., Acosta, L., 2018. Improving odometric accuracy for an autonomous electric cart. Sensors (Switzerland) 18 (1). doi:10.3390/s18010200.
UK-Government, 2018. Automated and Electric Vehicles Act 2018. Technical Report. UKAct2018.
UNECE, 2016. Proposal for Draft Guidelines on Cyber Security and data Protection Submitted by the Informal Working Group on Intelligent Transport Systems / Automated Driving*. Technical Report. UNECE.
UNECE, 2019. Revised Framework Document on Automated/Autonomous Vehicles. Technical Report. UNECE. https://undocs.org/ECE/TRANS/WP.29/2019/34/REV.2
UNECE, 2020. R155. Technical Report. UNECE.
UNECE, 2020. R156. Technical Report. UNECE.
Upstream Security, 2018. Global Automotive Cybersecurity Report 2019. Technical Report. Upstream Security.
Van Wyk, F., Wang, Y., Khojandi, A., Masoud, N., 2020. Real-time sensor anomaly detection and identification in automated vehicles. IEEE Trans. Intell. Transp. Syst. 21 (3), 1264–1276. doi:10.1109/TITS.2019.2906038.
Veitas, V. K., Delaere, S., 2018. In-vehicle data recording, storage and access management in autonomous vehicles. arXiv (May).
W3C. Documents published at W3C. https://www.w3.org/standards/types#eddraft-note.
Wan, Z., Guan, Z., Zhou, Y., Ren, K., 2019. Zk-AuthFeed: how to feed authenticated data into smart contract with zero knowledge. In: Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019, pp. 83–90. doi:10.1109/Blockchain.2019.00020.
Wang, F., Xu, Y., Zhang, H., Zhang, Y., Zhu, L., 2016. 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans. Veh. Technol. 65 (2), 896–911. doi:10.1109/TVT.2015.2402166.

Wang, Y., Masoud, N., Khojandi, A., 2019. Real-time sensor anomaly detection and recovery in connected automated vehicle sensors. arXiv 21 (3), 1264–1276. 10.1109/tits.2020.2970295

Wang, Y., Wu, X., Hu, D., 2016. Using randomized response for differential privacy preserving data collection. In: CEUR Workshop Proceedings, vol. 1558.

Wu, L., Fan, J., Xie, Y., Wang, J., Liu, Q., 2017. Efficient location-based conditional privacy-preserving authentication scheme for vehicle ad hoc networks. Int. J. Distrib. Sens. Netw. 13 (3). doi:10.1177/1550147717700899.

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

Xu, W., Yan, C., Jia, W., Ji, X., Liu, J., 2018. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. IEEE Internet Things J. 5 (6), 5015–5029. doi:10.1109/JIOT.2018.2867917.

Yan, C., Xu, W., Liu, J., 2016. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. DEFCON 24 (8), 109.

Zarouk, Y., Souici, I., 2013. Privacy protection in video surveillance system using enhanced evolutionary encryption algorithm. In: 2nd International Conference on Signal, Image, Vision and their Applications, SIVA'2013. Researchgate.

Zeng, K., Tech, V., Liu, S., Shu, Y., Research, M., Wang, D., Li, H., Dou, Y., Wang, G., Yang, Y., 2018. All your GPS are belong to us: towards stealthy manipulation of road navigation systems. In: Proceedings of the 27th USENIX Security Symposium.

Zhang, T., Antunes, H., Aggarwal, S., 2014. Defending connected vehicles against malware: challenges and a solution framework. IEEE Internet Things J. 1 (1), 10–21. doi:10.1109/JIOT.2014.2302386.

Zhang, T., Zhu, Q., 2018. Distributed privacy-preserving collaborative intrusion detection systems for VANETs. IEEE Trans. Signal Inf. Process. Netw. 4 (1), 148–161. doi:10.1109/TSIPN.2018.2801622.

Zorz, Z., 2018. Researchers hack BMW cars. https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/.

Meriem Benyahya Research assistant and Ph.D. candidate at the ISI, University of Geneva. She graduated with an Engineering degree from the Al Akhawayn University in Ifrane, Morocco and also received certification on Project Management from Temple University in Tokyo, Japan. Currently, she works on cybersecurity and data privacy implications and risk assessment tasks on Horizon2020 projects (AVENUE, nIoVe, and SHOW) which are focusing on the domain of automated vehicles. Professionally, she successfully managed IT projects from different fields and businesses, including PCI-DSS certifications, data centers infrastructure migrations, change management, IT master plans and business continuity plans/disaster recovery.

Anastasija Collen Scientific collaborator and Ph.D. candidate at the ISI, University of Geneva. She is an experienced R&D Engineer with a strong knowledge of web oriented and mobile technologies, focusing primarily on the fields of privacy and security. She is a member of the director board of InfoSec, 'continuous education' in information security program. She has contributed to several EU-funded ongoing projects including AVENUE, GHOST and nIoVe. Her current interest is in the development of the cyber security solutions for IoT devices, smart homes and smart cities infrastructure.

Sotiria Kechagia (LL.M.) works as a scientific collaborator with the Center for Digital Trust (C4DT), EPFL and the faculty of law of the university of Geneva. She is an experienced Legal Counsel with a demonstrated history of working with the private and public sectors. She is skilled in International Law, Medical Law, Bioethics, Data Protection Law, Cybersecurity, and Intellectual Property Law. Her academic interests focus mainly on the legal and the ethical challenges posed by the deployment of new technologies such as the Artificial Intelligence in various sectors (Health, Transport etc).

Niels Alexander Nijdam Computer scientist and senior lecturer ("Maître d'enseignement et de recherche") at the ISI, University of Geneva and is leading the Information Security group (I-Sec lab). He obtained his Ph.D. in computer science from the University of Geneva, MIRALab, where his topics included collaborative systems, distributed networking, remote simulations & rendering and programmable graphics. He worked on several research projects funded by a variety of European and Swiss funding programmes such as FP6, FP7, H2020, Marie-Curie, AAL as well as SNSF and CTI funded projects and has an active role in contributing to and shaping research proposals. He is currently coordinating the scientific efforts in H2020 AVENUE, SHOW and nIoVe projects.