Review and Perspectives on the Audit of Vehicle-to-Everything Communications

Chaima Zidi, Patrick Sondi, Nathalie Mitton, Martine Wahl, Ahmed Meddahi

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 July 2023, accepted 25 July 2023, date of publication 2 August 2023, date of current version 9 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3301182

TOPICAL REVIEW

Review and Perspectives on the Audit of Vehicle-to-Everything Communications

CHAIMA ZIDI[1,2], PATRICK SONDI[2], NATHALIE MITTON[3], MARTINE WAHL[4], AND AHMED MEDDAHI[2]

[1]LISIC—EA 4491, Université Littoral Côte d'Opale, 62228 Calais, France
[2]Centre for Digital Systems, IMT Nord Europe, Institut Mines-Télécom, 59000 Lille, France
[3]Inria, 59650 Villeneuve d'Ascq, France
[4]COSYS-LEOST, Université Gustave Eiffel, 59650 Villeneuve d'Ascq, France

Corresponding author: Patrick Sondi (patrick.sondi@imt-nord-europe.fr)

This work was supported in part by the Inria, Université du Littoral Côte d'Opale; and in part by the Pilotage Connecté et Agile des Opérations SDIS (PICADORS) Project which involves Institut Mines Telecom (IMT) Nord Europe.

ABSTRACT The connected vehicle is becoming a reality, and both centralised applications provided through telecommunication infrastructure, and cooperative applications achieved directly by the vehicles through vehicle-to-vehicle communications are gaining a lot of interest from the public. Though several solutions have been investigated to ensure identification and privacy protection of vehicles participating in these applications, only a few works address the recording of exchanged messages from an audit perspective, especially in the context of vehicle-to-vehicle communications only. This paper, proposes a review of the literature on vehicular communications, and explores particularly the solutions envisaged for audit in this context, such as the Blockchain technology. We also point out the most challenging issues that should be addressed in order to achieve an effective deployment of this latter in vehicular communications, especially in the vehicle-to-vehicle communication context, which should help in developing an effective Blockchain-based audit strategy.

INDEX TERMS Vehicle-to-everything communications, vehicular network security, users' privacy, electronic communication audit, vehicular communication accountability, vehicle misbehavior reporting.

I. INTRODUCTION

One of the most important and promising components in Intelligent Transport Systems (ITS) is the Vehicle-to-everything (V2X) communication paradigm. Equipped with wireless communication capability through an appropriate device (on-board unit - OBU, smartphone, etc.), the vehicle can communicate with every equipped entity around, such as nearby pedestrians (vehicle-to-pedestrian - V2P), neighbouring vehicles (vehicle-to-vehicle - V2V), surrounding road-side units (RSUs) (vehicle-to-infrastructure - V2I) or other devices (vehicle-to-device - V2D). All these interactions open the way to a wide variety of applications mainly intended mainly to improve road traffic safety, driver comfort, and vehicle smart driving in their environment [1], [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood.

To enable and supply all these innovative applications with the appropriate quality of service, the vehicles are empowered by a variety of new wireless communication technologies, such as the 5^{th} generation of cellular technology (5G), Visible Light Communications (VLC), and Millimeter Waves [3].

However, the messages exchanged in the context of these applications often contain sensitive information, such as the vehicle's or driver's identifier, the vehicle's position, speed, direction, status, and also various information related to life-threatening events. This latter information, which is accurate and timely, can significantly help by improving traffic flow and safety, and thus, most importantly, by saving lives. Unfortunately, in some of these applications, the messages are typically not encrypted and transmitted over short duration connections established between ephemeral participants [4]. In such open and dynamic communication system, these messages offer a gateway to malicious entities which may

hijack the application for their illegitimate actions. For example, they can disseminate erroneous information (fake accident, fake emergency break or fake traffic jam) which misleads other vehicles, and consequently modifies their behaviour (slowdown, emergency brake or reroute) in a risky way for other vehicles. These malicious entities can also use eavesdropped information to create detailed mobility patterns which potentially endanger the drivers' privacy. Indeed, a mobility pattern or model is a sequence of spatiotemporal records of a given user. Several location-based attacks use these data to anticipate user's moves, and extract user's Points of Interest (PoI) such as home, workplace or to infer social relationships (e.g., friends, coworkers, etc.) [5]. The consequences may therefore be catastrophic for road users [4], [6], [7], scaring them away from participating in cooperative applications.

Due to their potential impact on the users' lives, V2X applications have stringent requirements in terms of integrity, confidentiality, availability and accountability. Accurate security mechanisms are first needed in order to guarantee these requirements, and protect V2X communications against any fraudulent or misleading use [8]. However, it is necessary that they are complemented with audit mechanisms in order to ensure the continuous improvement of the security solutions, on one hand, and provide with accountability, on the other [9]. Audit refers to a set of investigation and evaluation operations allowing both to identify the security vulnerabilities in order to reinforce them, and to point out the fraudulent actions in order to identify the actors. It is based on a documented preliminary fieldwork process or event recording, gathering information from the V2X system in order to monitor the messages and all the events occurring, as well as the entities involved or their neighbours as suspicious events. Thus, it aims to provide evidence of the actions committed which are likely to be prosecuted, and therefore to determine the responsibilities which are incumbent on the various actors. Several research works studying the reputation of vehicles participating in V2X communications state that malicious vehicles or entities could be recognized, and therefore excluded in real time, so that they can no longer be able to participate in communications [10], [11]. However, malicious entities may have already committed actions likely to be pursued. Therefore, audit is very important since it not only facilitates the arbitration and the resolution of legal issues in case of suspicious events, but it also helps legislators regulate the use of the V2X system, anticipating its popularization.

Some applications (such as Waze,[1] Coyote,[2] TomTom,[3] for instance) mainly rely on an identified third party entity (such as the service provider, the car manufacturer, the application editor) which is responsible for providing the data necessary for the audit. These applications rely on V2I communications in which RSUs play a key role in linking the identified third party to vehicles by relaying information from and to vehicles. However, in case of collaborative applications in which messages are exchanged directly between the vehicles through V2V communications, the direct intervention of a third party is not guaranteed [12]. The absence of a third party, notably responsible for the verification of the broadcast information's coherence, increases the risk of propagating erroneous massages. Indeed, the context of collaborative applications is more vulnerable to attacks and more demanding for the distributed recording of events used by audit mechanisms. In addition, carrying out an audit of a communication system necessarily involves the processing of private and confidential information, which is subject to protection. Thus, in order to guarantee the audit's effectiveness and acceptance, it is important to set up a delicate balance between gathering data for audit and protecting users' data privacy.

An emerging technology which is gaining a lot of attention, the blockchain, stands out in such scenarios due to its immutability property, and its distributed nature. Composed of bound blocks, blockchain is a form of distributed ledger technology which uses cryptography concepts and tools, communication technologies, distributed systems and game theory. It also consists in consensus functions and reward structures and has great perspectives in various application areas of the vehicular networks such as data sharing, intelligent transportation systems, crowdsensing/crowdsharing, etc. Anonymity, transparency, seamless authentication, distributed and secured data storage are all blockchain functionalities which vehicular communications need for security, notably for their audit [13]. Recently, many blockchain-based security solutions have been proposed for vehicular communications [13], [14], [15], and some have even reached the market, such as VINchain,[4] which uses blockchain to provide a decentralized vehicle history by VIN (Vehicle Identification Number) for secured data transfer.

The objective of this work is twofold. First, we aim to present an overview of vehicular communication characteristics, including communication modes, wireless and mobile technologies, application profiles and evaluation tools. We will address the evolution of modern vehicular communications over the past few years to empathize its implication in recent security solutions proposed in this context. Then, we aim to review and discuss the main proposals of the literature regarding event recording solutions for the audits which have been or could be used in the context of vehicular communications. The discussion at the end will highlight the topics which can direct future research into ensuring the audit of V2X communications.

A. SURVEYS ON V2X COMMUNICATION AUDIT

Several research papers address security-related issues in vehicular communications, and provide an analysis of existing solutions. Most of them have investigated V2X

[1] https://waze.com
[2] https://moncoyote.com
[3] https://tomtom.com
[4] https://vinchain.io

communication security from different perspectives, such as attacks, security requirements and countermeasures. Among the surveys addressing security issues in V2X communications [2], [6], [8], few papers analyse their audit precisely. In [7], the audit is mentioned among the security requirements along with non-repudiation, and considered as being of the utmost importance in the context of accident scenarios in order to determine their real causes. Other papers focus on the behavioural aspects of the nodes, and the network architecture characteristics regarding security [16], [17], [18], [19]. In [20], the authors analyse the main factors of defence systems against attacks. One of these factors is the source of the data analysed by the system. The data source can be the logs/audit trails of the in-vehicle system, the applications or network traffic. Among the surveys which address the use of blockchain in V2X communications [13], [14], [21], the authors of [15] underline the key role of the blockchain in the implicit provision of security requirements, especially in the implementation of public auditing through its immutability property. Each block created can be independently verified by every node in the blockchain network. Table 1 summarizes the most relevant features of existing survey and review papers, and highlights the main enhancements in this paper.

B. MAIN CONTRIBUTIONS OF THIS WORK

This work is built upon recent research in vehicular communications security to present a state of the art of the works published so far on audit. More precisely, we mostly cover publications from the last ten years. The objective is to point out the system vulnerabilities and security limitations, aiming to show the importance of audit solutions. We analyse current trends in V2X communications and their impact on security with the aim of pointing out the need for an audit system, especially for collaborative applications. While studying all existing audit approaches, we particularly focus on the use of the blockchain technology in V2X communication auditing. Our contributions can be summarized as follows:

- We present a V2X review aimed at covering recent advances in vehicular communications. Specifically, we analyse key aspects of V2X evolution, including communication modes and technologies. We enumerate the most innovative vehicular communication applications and present existing simulation and testing tools dedicated to vehicular communication evaluation.
- We introduce emerging technologies bringing new trends in vehicular communication security.
- We propose an analysis of current audit solutions in V2X with the aim of identifying the missing elements needed for an effective event recording system. The objective is to draw the guidelines for prospective work on the use of blockchain for audit in V2X communications.

The remainder of this article is organized as follows. An overview of vehicular communications is presented in section II. Existing frameworks for securing V2X communications are enumerated and analysed in section III, in which we provide an overview of the current trends in security, notably the blockchain technology. Section IV introduces the audit through its different stages and presents a state of the art on auditing in vehicular networks. In section V, we discuss the main criteria challenging the design of an event registration system prior to the audit procedures in V2X communications. Finally, section VI concludes the paper.

II. AN OVERVIEW OF V2X COMMUNICATIONS

In recent years, technological advances –in wireless communications as well as in automotive equipment– have spawned a new generation of connected vehicles, ushering in a new era in vehicular communications. More powerful than in the vehicular ad hoc networks (VANETs), vehicles are now able to communicate, not only with other vehicles and the network infrastructure, but also with many other communicating things, thus defining the so-called Vehicle-to-everything (V2X) system. Together with the prolongedly used Dedicated Short-Range Communication (DSRC) technology, many communication technologies, such as cellular technologies, have been developed and evolved to allow V2X communications and sustain the broad capabilities of the connected vehicles.

The evolution of vehicular communication technologies has enabled a plethora of innovative applications ranging from passengers' entertainment to autonomous driving, and including driver assistance. Intelligent Transport Systems (ITS) are one of the advanced applications of V2X, providing new services to road users for safer and optimal journeys. Like other technologies for vehicles, V2X protocols and standards must be validated before being operational in the real world. A common tool for protocols' validation and performance evaluation is the simulation tool. In this section, we present a review of V2X communication modes and technologies, some applications for this context, and different simulation tools dedicated to their evaluation.

A. COMMUNICATION MODES AND ARCHITECTURE

V2X is the future of vehicular communications and it encompasses communications between the vehicle and all the entities around it, likely to interact with the vehicle. These entities can be vehicles, pedestrians, network infrastructures, an electrical network, or any other communicating device [4], [17].

When only considering the VANET, V2X communications consist in vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications. A VANET is an ad hoc network which relies on a homogeneous network technology (IEEE 802.11p or LTE-PC5 as an example, section II-C) and in which communications are limited to the size of that network. But, when considering Internet of Vehicle (IoV), which is when vehicles are connected to the Internet and act as an ad hoc network [22], V2X communications are related to any IP communication between at least a vehicle

TABLE 1. A compararison of the most recent V2X security related surveys or reviews.

Paper	Year	Security requirements	Privacy requirements	Attacks' classification	Authentication techniques	Pseudonym lifecycle	Blockchain-based techniques	ML-based techniques	Audit definitions & techniques	Major contributions
[8]	2018	✓		✓	✓					A review of anonymous authentication schemes, location privacy protection mechanisms and trust management models in VANETs.
[14]	2020		✓		✓		✓			A review of the blockchain-based cybersecurity mechanisms for secure communication, privacy protection, trust and authentication.
[7]	2020	✓		✓	✓					A comparative analysis of cryptographic security schemes, trust management schemes based upon discrete characteristics and intrusion detection systems.
[6]	2020	✓		✓						An analysis of various possible attacks and preventive measures.
[2]	2020	✓		✓	✓					An analysis of the security challenges, attacks and requirements in V2X.
[18]	2020	✓		✓	✓					A review of some major security attacks on intelligent connected vehicles and some of the available defence mechanisms such as cryptography, network security, software vulnerability detection, and malware detection.
[16]	2021	✓		✓	✓			✓		An analysis of recent security solutions' strengths, limitations and key challenges.
[20]	2021	✓						✓		A description of the in-vehicle system architecture, security issues and vulnerabilities. An overview of different malware types, and a classification of the available defence techniques against malware.
[19]	2021			✓				✓		A survey of misbehaviour detection mechanisms in cooperative networks.
[13]	2022	✓		✓			✓			A review on the existing security solutions using blockchain in VANETs.
[17]	2022	✓		✓						An overview of V2X security issues, challenges, and countermeasures.
[15]	2022	✓	✓	✓	✓		✓			A survey of the characteristics of blockchain and its use, especially in security and privacy in VANETs.
[21]	2022	✓		✓			✓			A comprehensive survey on different vehicular applications using blockchain technologies.
this paper	2023	✓	✓		✓	✓	✓		✓	An overview of the current trends in V2X security showcasing auditing and its techniques as futuristic mechanisms for security sustainability.

and an object. V2X communication modes can therefore be one of the following, among other: vehicle-to-cloud (V2C) or vehicle-to-network (V2N) when connecting with an Internet of Thing (IoT) interface, V2I or Vehicle-to-roadside (V2R) when communicating with a road side unit (RSU), vehicle-to-pedestrian (V2P) or vehicle-to-device (V2D) when linking to vulnerable road users (VRU) or vehicle-to-sensors (V2S) and V2V when establishing connection with an on-board unit (OBU) [22]. In terms of communication architecture, IoV can be considered as a huge network composed of several heterogeneous network connected to clouds [23]. In short, V2X brings together several modes of communication, whose

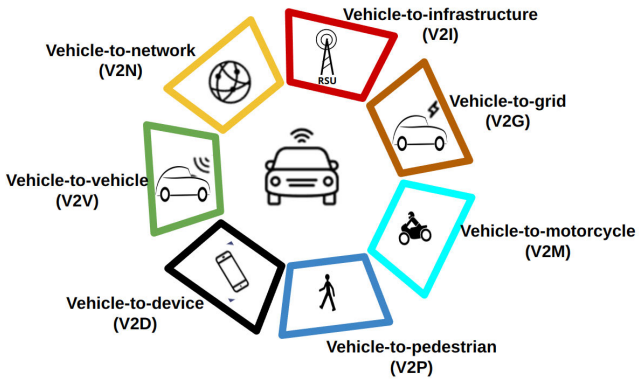


FIGURE 1. V2X communication modes.

acronym is defined according to the type of counterpart with which the vehicle communicates [24]. Figure 1, the following V2X communication modes are listed:

- Vehicle-to-Vehicle (V2V) which relates to the direct communication between vehicles. In particular, V2V communication mode allows vehicles to broadcast data in their surroundings which are required for safety collaborative applications, such as their location, speed, heading, etc.
- Vehicle-to-Infrastructure (V2I) which relates to the direct communication between the vehicle and the road infrastructure equipment (RSU: road side unit), such as traffic lights and surveillance cameras.
- Vehicle-to-Network (V2N) which represents the communication between the vehicle and the cellular infrastructure, such as a base station or its variations according to the different technologies.
- Vehicle-to-UAV (V2U) in which Unmanned Aerial Vehicles (UAV) are used to extend the coverage areas of communication to relay it between vehicles in an out-of-coverage area (communication in infrastructureless area) [25].
- Vehicle-to-Pedestrian (V2P) in which different types of media help communication between the vehicle and the pedestrians such as smartphones, canes for the visually impaired, strollers, lights and bike navigators. V2P communication aims to enhance vulnerable people's security by conveying alert in times of any hazardous situation. Vulnerable people include pedestrians as well as bike riders, scooter users, wheelchair users, etc.
- Vehicle-to-Motorcycle (V2M) which represents the communication between the vehicle and motorcycles to prevent collisions, thus decreasing a death casualty [26]. V2M paradigm is widely discussed in the 2022 report edited by the Federal Highway Administration (FHWA) of the United States of America about the use of technology for motorcycle safety [27]. Though a motorcycle is considered as fragile as a bicyle or a pedestrian, it can also move as fast as a car, which justifies it as a specific sub-case.
- Vehicle-to-Device (V2D) in which the word "device" or equipment refers to a smart device such as a smartphone, smart key or tracking equipment.
- Vehicle-to-Grid (V2G) in which the word "grid" represents the electrical power supply network. Vehicle-to-Grid (V2G) where the "grid" stands for "power grid" and "vehicles" are plug-in electric vehicles [28]. The aim of a V2G system is to allow bidirectional power flow to faster charging vehicles, but also to provide services to the grid such as drawing and redistributing the energy stored in the battery of an electric vehicle to the power grid [29].

The interconnected entities of the V2X system can be organized into three domains, as depicted in figure 2: the intra-vehicle, the inter-vehicle and the Cloud domain. This structure which defines the high level architecture of ITS [3] can be described as follows:

- The intra-vehicle domain includes all the sensors and electrical components located inside the vehicle. They are managed by the Electronic Control Units (ECUs) controlling a wide range of automobile functions including powertrain, vehicle safety, in-vehicle infotainment, comfort control [30]. ECUs communicate through bus communication networks such as the Controller Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Media Oriented System Transport (MOST) and Ethernet. Different in cost, bandwidth, and access control, the use of each bus network technology depends on timing requirement and the criticality of the target automobile function.
  Intra-vehicle domain communications are essential to control the in-vehicle equipment, and to detect and analyse problems with drivers and their vehicles in order to minimize accidents due to drowsiness or vehicle malfunction [31]. A key component of a vehicle which coordinates the various ECUs and manages bus communications, the gateway ECU, also known as an On-Board Unit (OBU), links communications to external networks.
- The inter-vehicle domain involves the roadside users (such as pedestrians, motorcycles…), the RSUs, the vehicle OBU which is responsible for the data collection and processing in addition to the interaction with surrounding entities. This domain covers the V2V, V2I, V2N, V2P, V2D, V2G and V2M communication modes. Various communication technologies can be used in this domain such as wireless and cellular standards, which will be reviewed in section II-C.
- The third domain, here identified as the Cloud domain, plays a central role in the modern vehicular environment as it allows the use of Cloud computing and Fog computing technologies. It encompasses multiple authorities which provide security services, and many servers which provide storage and computing services. Thanks to the services of this domain, the V2X system offers a multitude of innovative applications which would not be

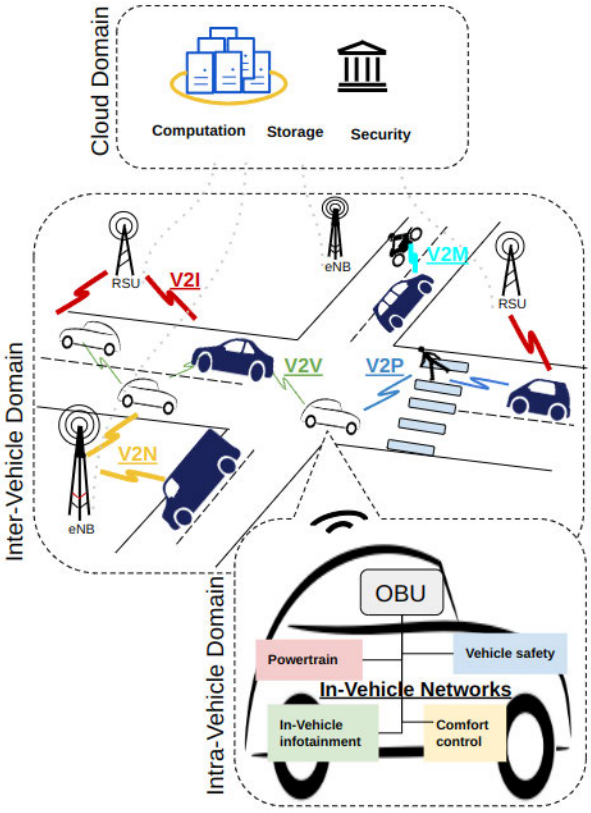


FIGURE 2. V2X High level architecture (inspired from [16]).

possible otherwise. Indeed, current applications require enormous computing and storage resources. With this domain, computing and storage are relocated in the Cloud, whose resources can be easily purchased or rented [32].

B. APPLICATIONS

The main purpose of the V2X technology is to improve the road safety and usage by reducing traffic congestion, and the number of accidents, as well as to preserve the environment by saving energy, while making efficient use of vehicle resources and taking advantage of smart road devices. Several innovative and ambitious applications arise [17], [33]:

- **Cooperative driving**, in which V2X technology can facilitate the collaboration of vehicles and any other entity with the aim of both minimizing the disruption caused by lane changes or sudden braking, and allowing the exchange of information in real time with panels and traffic lights. Applications - such as ego-localization which allows vehicles to share their position information and uses that of their neighbours in order to enhance their own position information, or collective perception thanks to which vehicles can share their Local Dynamic Map (LDM) of the road traffic with the vehicles entering the road section - are two representative examples [34].
- **Platooning**, in which V2X technology can help the safe formation of a convoy in which the vehicles are very close together [35], which makes it possible to optimize the use of road space, to save fuel and to make transport of goods more efficient.
- **Traffic jam warning**, in which V2X communications are used to warn vehicles of traffic jams or roadworks, so that they can slow down smoothly, and avoid hard braking [36].
- **Collision avoidance**, in which V2X communications allow vehicles to broadcast information such as identity, position, speed and direction, which can be combined with other vehicles' data to create a local map of the surroundings in real time to alert of any potential collision [37].
- **Hazard warning**, in which V2X technology can be used to expand a vehicle's electronic field of vision, to detect hazards around a blind spot, or obscured by the fog or other obstacles, such as heavy vehicles [34].
- **Autonomous driving and remote control**, in which V2X technology, in conjunction with other sensors and communication systems, can enable vehicles to become autonomous, which can be useful for long distances or in case of temporary driving incapacity [38].
- **Advanced Driver Assistance Systems (ADAS)**, in which V2X communications supply information to augmented reality systems to provide a real-time dashboard or head-up navigation [39].
- **Infotainment**, in which V2X communications can enable a seamless Internet connectivity to access web-related applications, audio-video streaming, and navigation services which can be used to find nearby medical shops, restaurants or gas stations [40].

C. COMMUNICATION TECHNOLOGIES

V2X communication technologies for collaborative ITS (C-ITS) are still developing. In order to exchange messages with their surroundings and meet the communication needs of both the road context and applications, V2X communication mainly relies on two types of networks, IEEE 802.11 and cellular networks (table 2). First, standards have been specified which enable to deal with applications whose latency requirements are within 100 ms. Recently, new technologies have been developed to cope with time-critical safety applications with latency requirements below 100 ms.

For applications with latency requirements within 100 ms, direct V2V, V2I and V2P links can be established with an IEEE 802.11p-based technology or with the LTE-V2X, operating in direct communication mode, within short range communication (inferior to 1 km). For V2N long range communication (superior 1 km), the 3^{rd} generation partnership project (3GPP) C-V2X release 14 (published in 2017) uses the cellular (or network) of the LTE technology [43]. C-V2X 3GPP release 14 enables to deal with low-bandwidth safety applications as well as high-bandwidth multimedia services [44].

TABLE 2. Some features of some ITS technologies in 2018 [41], [42].

V2X Technology	802.11p			cellular
Known in literature as	DSRC/WAVE	ETSI ITS-G5	ARIB STD-109	3GPP LTE-V2X (or C-V2X 3GPP Release 14)
Standard [41]	IEEE 802.11-2012, IEEE 1609.2 - .4, SAE J2735 and SAE J2945/x series	"ITS-G5", ETSI ITS series	ARIB STD-109	3GPP TS 22.185, TS 23.285 for V2X and LTE, and TS 36 series for radio access
(Region)	(USA)	(Europe)	(Japan)	(Global)
Vehicular networking	V2V, V2I, V2P	V2V, V2I, V2P	V2V, V2I, V2P	V2V, V2I, V2P, V2N
Radio performance [42]				
Max. radio coverage	1000 m (with LOS)	1000 m	1000 m	1000 m
Max. data rate	27 Mbit/s	27 Mbit/s	18 Mbit/s	27 Mbit/s
Max. packet size	2 Kbytes	2 Kbytes	100 bytes (from veh.); 1500 bytes (from infrastructure)	2 Kbytes
Latency	within 100 ms	within 100 ms	within 100 ms	within 100 ms; 1000 ms for V2N

IEEE 802.11p amendment [45] has been part of the 802.11 standard since 2010. It enables both vehicle-to-vehicle (V2V) communication and vehicle to RSU communication (V2I) (figure 2). Based on the IEEE 802.11p standard, the European Telecommunications Standards Institute (ETSI) specified the access layer technology (the physical layer and media access control) named ITS-G5 [46] (table 2). In the United States, the Dedicated Short-Range Communications (DSRC) protocol was developed using IEEE Wireless Access in Vehicular Environment (WAVE) standards which follows IEEE 1609.x standards as DSRC MAC layer and IEEE 802.11p as the lower layer [47], [48]. 802.11p technologies support a 252 km/h relative speed between communicating nodes. Both DSRC and ITS-G5, also direct LTE-V2X, operate in the 5.9 GHz band in Europe or the US. In distributed mode (also referred to as direct, PC5 or sidelink mode), "PC5" communication interface of LTE-V2X is independent of the cellular network and competes with ITS-G5. In controlled mode (also referred to as cellular network), a control signalling exchange between a cellular antenna and each of the communicating vehicles is established for any V2V link via the Uu interface of the communication devices. V2V, V2I, V2P exchanges use the distributed communication mode while V2N uses the C-V2X controlled mode.

Applications such as those of vehicle platooning, advanced driving, extended sensors and remote driving require low latency (under 100 ms and even below 10 ms) and high reliability (90-99.99%) quality of service [43] which cannot be guaranteed with the technologies listed in table 2 [34], [43]. For those low latency, high reliability applications, a new radio (NR) cellular V2X technology (3GPP NR-V2X) has been specified in C-V2X release 16 and published in 2020. As LTE-V2X, NR-V2X has two modes of resource allocation, the centralized NR-V2X mode in which a generation mode (gNB) schedules the radio resources and the decentralized NR-V2X mode thanks to which vehicles select radio resources on their own [43]. Comparing to C-V2X 3GPP release 14, enhancements provided by release 15 aim to achieve longer range, higher density, very high throughput and reliability, wideband ranging and positioning in addition to very low latency [44]. Also, in order to handle with these low-latency applications, the IEEE 802.11bd task group has been developing an amendment of the IEEE 802.11 standard since January 2019. 802.11bd will operate in the 5.9 GHz band and 60 GHz, support relative speed of vehicles going up to 500 km/h and allow a data rate two times better than 802.11p [43]. Several papers explain the evolution of the current and upcoming technologies. As an example, [44] compares C-V2X and DSRC focusing on enabling vehicular safety for longer range and consistent performance in congested situations. It explains that C-V2X can achieve line-of-sight V2V ranges of 443 versus 240 m for DSRC and non-line-of-sight V2V ranges of 107 m versus 60 m for DSRC, which has an impact on the awareness time during dangerous situations. The recent 802.11bd and NR-V2X evolution of radio technologies can be read in [49]. Reference [50] proposes a tutorial on 5G NR-V2X communications and notably explains the coexistence mechanisms between 5G NR-V2X and LTE-V2X.

In terms of messaging, both ETSI ITS and SAE J2735 DSRC standards define the syntax and semantics of V2X messages. Basic messages for safety application are, on one hand, the Basic safety message (BSM) specified in SAE J2735 and, on other hand, both the Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Message (DENM) specified by ETSI ITS. BSM as

CAM messages allow every communicating node to maintain awareness of nodes in their direct neighbourhood. A BSM is a periodic message broadcasted at a maximum rate of 10 Hz. It is a two-part message in which the first part is fixed size and conveys a DSRC message identifier and inner information about the transmitting vehicle (position, motion information, brake system status and vehicle size). A BSM can include a second part of variable size which consists in vehicle safety extensions and which is related to event information such as emergency braking, traffic jams, etc.) [51]. ETSI ITS specifies Cooperative Awareness Message (CAM) which are periodically sent and Decentralized Environmental Notification Message (DENM), whose transmissions are triggered by events. A CAM message contains status information of its sending station such as time, motion and position and attributes information on the sending node such as its dimensions [52]. DENM, sent upon detection on an event related to road hazard, driving environment, or traffic condition, is used to describe it [53].

D. EVALUATION AND TESTING TOOLS

Real world deployment of V2X system at a large scale is still rare, and most of the applications are still proposed through vehicle OBU (safety applications), and driver's smartphones (infotainment applications) while relying on cellular communications and without direct cooperation between the vehicles. Therefore, most of the experiments, at a large scale, on V2X applications involving many vehicles could be very expensive due to customized vehicles and road infrastructures. Some research projects such as SCOOP[5] have tried to perform real-world testing. However, though the experiments covered a large area thanks to the cooperation of different partners across Europe, only few scenarios involving few vehicles have been actually realized. Therefore, simulation remains the best alternative to reduce testing expenses and easily validate theoretical features of V2X communications and security before implementation or standardization [3], [61]. Most of the existing simulators used in V2X system evaluation focus either on modelling mobility patterns, or on modelling telecommunication infrastructure, communication protocols and vehicular applications [62]. Examples of mobility simulators include SUMO [63], VISSIM [64], SimMobility [65], PARAMICS [66], and CORSIM [67]. Examples of available network simulators available (some of them widely used in VANETs) include OMNeT++ [68], OPNET [69], JiST/SWANS [70], NS3 [71], and NS2 [72]. A simulator for vehicular environment is then usually the combination of network and mobility simulators. An ideal simulator should closely reflect the real behaviour of vehicles in road traffic, while interacting with other entities. In addition to the mobility pattern, a simulator should be based on a network model which describes the components of the communication system, relevant metrics such as the packet error rates or the end-to-end delay, and eventually the events.

However, as vehicular communication technologies are evolving very rapidly, most of the available tools focus on a particular technology and the integration of other technologies, especially the new ones, can be a long and challenging task [3]. Therefore, designing and developing a realistic simulation tool for real road traffic and vehicular communications with modern technologies support is considered as an important research and engineering area. The same applies to modelling vehicular applications network flows, and vehicles road traffic in the simulators in order to test and validate security mechanisms. Several attempts to model and verify routing and security protocols using formal tools have been proposed. A tool such as Rodin allows modeling a vehicular environment including node mobility and communications [73], and also to verify and validate security protocols [74]. These attempts may lead to new evaluations tools to validate security mechanisms in the context of V2X communications. In Table 3, inspired from [62], we provide a summary of the features of the newest and most popular simulators for vehicle networks and verify their support to new technologies (such as Software Defined Networking (SDN), edge computing, etc.) and security services. A detailed analysis and comparison of the latest versions of simulators can be found in [62].

Most of these simulators now allow modelling devices with processors and storage, in addition to network interfaces, which makes it possible to model and evaluate complex applications such as a blockchain-based audit system.

III. SECURITY AND PRIVACY IN V2X COMMUNICATIONS

Securing vehicular communications is essential considering that malicious intruders can access and use confidential and private information for dangerous and sophisticated attacks such as Sybil attacks, distributed denial-of-service (DDoS), etc. A classification of attacks based on severity level and other criteria (such as attacker model, compromised security requirements, layer…) can be found in this article [75]. Those attacks mainly threaten the data security services such as authentication, integrity, availability, confidentiality and their performance as represented in figure 3 and discussed in the following. Usually referred to as security requirements or services, they represent what V2X systems need to make sure of by a security mechanism in order to function correctly, and to be publicly reliable and accessible. They are typically viewed as the primary goals of any security infrastructure. A classification of attacks according to such security requirements is presented in [6] and [76].

Privacy is also a paramount security requirement in the vehicle environment [77], despite the fact that it is addressed differently depending on the countries [78]. Some countries may require and impose a mandatory privacy policy in the transportation system to be publicly deployed. They consider

[5]https://www.scoop.developpement-durable.gouv.fr

TABLE 3. Summary of the features related to security evaluation in the most recent simulation tools.

Simulator	Network simulator	Mobility simulator	Support for new technologies	Support for security services	Newest release	License
NetSim [54]	-	SUMO	SDN, 5G	Authentication, confidentiality [55]	2021	proprietary
Veins [56]	OMNeT++	SUMO	SDN, Edge computing, 5G, self-driving cars	Authentication, confidentiality, integrity, availability, non repudiation, privacy [57], [58], [59]	2020	open-source
Eclipse MOSAIC [60]	OMNeT++, NS-3	SUMO & VISSIM	5G, self-driving cars	Authentication, confidentiality, integrity, availability	2020	open-source

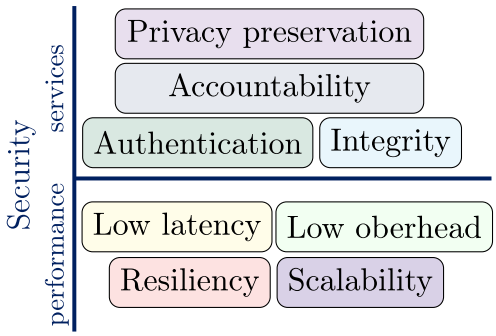


FIGURE 3. Security design requirements and services.

that preserving users' privacy is as important as safeguarding their lives. While other countries agree that full identification of drivers is compulsory regardless of the danger related to privacy breaches such as tracking or profiling. Therefore, privacy is approached separately [79] from the other security requirements.

An aspect separating security from privacy is the conflict between their respective accountability and anonymity requirements [80]. Indeed, full anonymity may allow misbehaviour occurrence as attackers would act maliciously without the fear of being identified. Nevertheless, it is possible to achieve both security and privacy requirements when designing a vehicular system by adopting conditional privacy, the main enabler of the audit process. As for the audit, it is considered as a security tool leading above all to accountability, one of the essential pillars of security.

Recently, a multitude of approaches to enhance security while preserving privacy have been proposed, notably based on new technologies such as homomorphic cryptography which is still under development [81], [82]. In the following, we first briefly review the security and privacy requirements/services. Then, a short review of recent approaches defending security in V2X communications with a particular focus on blockchain-based solutions is provided, as well as a discussion aiming at positioning auditing in relation to security solutions is provided.

A. SECURITY AND PRIVACY OBJECTIVES

Security is important in wireless networks to ensure a number of requirements which guarantee the protection of the entire system: the communication as well as the participants. However, the unique characteristics of vehicular environments in vehicular networks impose several new requirements [83]. Hereinafter, we list the main requirements highlighted by most articles [78], [83], [84].

- Authentication or entity authentication ensures the legitimacy of the entity participating in the communications. Attacks on authenticity allow illegitimate entities to gain unauthorized access to private information such as in sybil attack, through stealing or falsifying identity of legitimate network members.
- Integrity or message authentication ensures that messages cannot be modified nor dropped. Attacks on integrity aim at altering and manipulating data in transit such as in replay attack, timing attack, bush telegraph, etc.
- Accountability ensures that entities are responsible for their actions, and that the law accounts them for their actions. It imposes non-repudiation mechanisms, and requires traceability.
- Non-repudiation involves that entities should not be able to deny, dispute or refute the authorship of the messages they sent. Man-in-the-middle is one of the attacks related to this requirement.
- Traceability ensures that only authorized authorities are able to trace the actions of entities, record and verify the history of events, and interconnect identities to entities.

The preservation of the entities' privacy can be fulfilled by relying on several concepts such as anonymity, pseudonymity, unlinkability, or unobservability as stated in [85]:

- Anonymity means that entities should be anonymous and indistinguishable among a group of senders. The main purpose of anonymity in the vehicular environment is to hide the long-term identity by using short-term identity or pseudonyms. It should guarantee the unlinkability and unobservability, and thus contribute to the protection of users' privacy.

- Conditional privacy ensures that the identity of a registered vehicle is not accessed, except by authorized entities when malicious activities are detected.
- Confidentiality prevents the disclosure of information to unauthorized entities.
- Minimum disclosure means that entities should reveal the useful minimum of their private information when communicating.

In addition, depending on the application needs, further requirements can be applied at the level of the security scheme itself, such as:

- Low overhead implies that the best security level should be achieved with the least number of computational resources and the lowest communication overheads possible for all the parties involved.
- Low latency implies that a security scheme should provide frequent, real-time information for time-sensitive applications such as security-related ones.
- Resiliency means that the security scheme must be able to maintain or recover quickly from damage caused by attacks.
- Scalablility entails that a security scheme should function without degradation regardless of the vehicle density (low, medium, high, time-variable) on the road.

In order to meet these requirements, several standards, projects and recommendations which consider the security and privacy aspects of V2X communications have been developed. Among the standardization authorities around the world, listed in [86], we can mention the European Telecommunications Standards Institute (ETSI), the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA), the Society of Automotive Engineers (SAE), the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and the CAR-to-CAR Communication Consortium (C2C-CC). In [84], the authors focus on security and privacy aspects of the European Union (EU) initiatives, such as past or present V2X-related EU projects, and analyse the specifications of ETSI, as it is the major active standardization organization in Europe.

Along with the efforts of standardization organizations, researchers are studying new technologies such as Blockchain to combat cybersecurity threats. The purpose of leveraging Blockchain technology is that it implicitly provides some of the aforementioned security requirements through its features such as decentralization, resistance to tampering, traceability, and most importantly, public auditing through its consensus mechanism. As such, in the following we examine some of the Blockchain-based techniques used to secure V2X communications.

B. BLOCKCHAIN-BASED SECURITY TECHNIQUES

The security solutions using blockchain in the literature can be split between solutions leading to authentication techniques and those leading to intrusion detection techniques.

1) AUTHENTICATION TECHNIQUES

Authentication is an important part of any security framework. It plays a key role in protecting vehicular communications from most attacks, especially those initiated by outside attackers (not authorized to operate in the network). It is used to easily identify rogue entities and fake messages.

Existing authentication schemes are mainly based on four major approaches [16]: public key-based approach, identity-based approach, group signature-based approach, and certificateless approach [87]. In the public key-based schemes, multiple public/private key pairs and a certificate-based signature are used for participants' authentication. In contrast, in the identity-based schemes, the identifier of a vehicle itself is used as the public key and to generate the private key [8]. The certificateless approach introduces a partial private key from which the actual private/public keys are indirectly generated so that vehicle privacy is not violated. Reference [80] reviews other existing authentication schemes and considers them in terms of capacity to fulfil security requirements, resistance to attacks, and performance (computational and communicational overheads). The schemes mainly suffer from high computational overheads which can degrade their performance [88], [89], [90].

To reduce the high computational and communication overhead of conventional authentication schemes, blockchain technology has been explored in the context of the current solutions. In [91], the authors propose a technical architecture for a decentralized vehicular Public Key Infrastructure (D-VPKI) in which they use blockchain in order to replace the central trusted authorities and provide a privacy preserving decentralized authentication. The authors discuss the design principles of D-VPKI, meeting ITS requirements, including vehicle identification, pseudonyms and revocation process. The authors also discuss the main challenges (such as governance) arising in such decentralized architecture, and propose alternatives benefitting from blockchain characteristics. To materialize D-VPKI, a proof of concept is presented while evaluating some hardware components and technologies for possible implementation.

In [92], a privacy-preserving authentication scheme for VANETs based on consortium blockchain is proposed. A prototype based on Hyperledger Fabric [93] is implemented to test and evaluate the performance of the proposed authentication framework. In [94] a blockchain based authentication is proposed using fog computing over cloud computing, and 5G and Beyond 5G technologies. The system architecture is composed of three layers, namely: a cloud layer, a fog layer, and the end devices layer. A customized Blockchain (BC) is used to store user-related data for authentication. Each block consists in a hash table which contains the public key of a user, and a hash value. The latter is calculated using the user's data and public key, and is then signed using the user's private key. The authors of [95] propose an anonymous re-authentication based on blockchain code and transaction number for secure handover at a lower cost. Table 4 summarizes the main features of some relevant

authentication mechanisms. In the literature, many recent and interesting blockchain-based authentication schemes have been published [96], [97], [98], [99]. They primarily try to provide strong, privacy-preserving authentication to ensure straightforward and secure vehicular communications. However, trust and reputation are still difficult to achieve through authentication [100].

2) INTRUSION DETECTION TECHNIQUES

Intrusion detection techniques are the second line of defence against cyberattacks. These techniques primarily work against insider attacks from authenticated users. They are based on rules and indicators of an established trust model, assessing the level of trust on system components. This is done primarily by monitoring the behaviour of nodes [101] and the transmitted data [76], [100]

Most of the techniques proposed for intrusion detection systems can apply to in-vehicle systems [102]. However, the growing size and complexity of vehicle networks lead to the need for more automated and decentralized solutions based on Blockchain to establish trust and detect intruders. In [57], the authors propose a blockchain-based collaborative revocation method using clustering. A Traffic Management Center (TMC) is responsible for community construction. Each vehicle disseminates CAM every 0.1 second. When receiving multiple CAMs, each vehicle constructs a list of stable surrounding vehicles and sends it to the TMC which processes the communities based on the graph rules, then issues and sends the community's start list with a cluster ID to each community head. For community detection, a proof of location is used between each pair of vehicles. Then, based on exchanged proofs of location, each vehicle constructs a matrix of detection which is used to identify and revoke malicious vehicles. A local blockchain is used to maintain each community step. The miner of the first step is the TMC which ensures that only community vehicles can communicate to create the genesis block which contains the smart contract. The second part of the blockchain registers the peer-to-peer proof-of-location. The miner in this part is the closest vehicle to all community vehicles. The third part registers the matrix of detection which combines the proof-of-location across the community. The Paxos consensus is used to agree on the matrix value in the last part of the blockchain, and then declare the malicious vehicle. The decision is based on the agreement of more than 50% of the community vehicles. The trust authority constructs the block and aggregates the agreement.

A consortium blockchain and smart contracts are used to ensure a trustworthy environment for secure data storage and sharing in [103]. They propose a three-layer architecture composed of a network layer, a BC edge layer, and the BC network layer. Practical byzantine fault tolerance (PBFT) is used to audit publicly, store shared data, and records the whole consensus process. In [59], a blockchain-based system for message rating credibility is used for trust management. Similarly, a message and vehicle trustworthiness using trust level in blockchain is proposed in [104]. In addition to blockchain-based techniques, a large number of studies explore the potential of machine learning in intrusion detection [18], [105], [106].

C. KEY COMMENTS

From this exploratory study of the literature on security in V2X communications, it is possible to draw an overall picture of the modern security techniques and technologies which are used. As classified in [16] and [19], security techniques can be either proactive or reactive.

Proactive techniques are preventive measures to mitigate potential attacks. This category of approaches includes authentication techniques which control access to the networks and services.

However, since those techniques are ineffective against internal attacks, the reactive techniques offer a solution to detect and react accurately to such attacks. These reactive techniques include intrusion and misbehaviour detection approaches, which detect and isolate anomalies, therefore limiting the impacts of the attacks.

Proactive and reactive techniques are complementary to produce an efficient shield against security issues. However, despite the significant efforts and the technological advances, vehicular systems and communications are still vulnerable. Indeed, the current automotive system incorporates new modern services and capabilities which improve users' comfort and enhance road safety. However, all the advantages brought by these modern technologies in vehicular system and communications come with new security vulnerabilities which can be exploited to compromise the services. These vulnerabilities can be primarily caused by software errors or flaws, or result from either the mobile communication technologies or the in-vehicle equipment and networks [16]. Therefore, a continuous vulnerability assessment service becomes a necessity to reinforce the security mechanisms already in use. This service could be provided through audit mechanisms.

IV. V2X COMMUNICATIONS AUDIT

Conducting an audit of a communication system can help maintain security practices, as well as create new security policies. Auditing can also help to detect security inefficiencies, and make sure that responsibility for a specific action could be unambiguously assigned to an individual user in a fair protocol. The necessity of auditing in vehicular networks arises from the possibility of misbehaviour among users. While attacks performed by outsiders can be addressed by means of authentication techniques, misbehaviour among legitimate network nodes is a more challenging problem to address [76]. Thus, auditing becomes paramount in detecting the undetected misbehaviour, by ensuring accountability and non-repudiation, and therefore by complementing the efforts of existing security solutions.

TABLE 4. Blockchain-based security solutions.

	Ref	Year	V2X modes	Topology	Main contribution	Evaluation platform	Performance & Limitations
Authentication	[91]	2021	V2N	-	A blockchain-based decentralized PKI with no central trusted authority	a Proof-of-Concept	proven conceptual feasibility however no qualitative nor quantitative evaluation of performance
	[92]	2020	V2I	-	A privacy-preserving authentication scheme for VANETs based on the consortium's blockchain, in which entity authenticity is represented by a new data structure transaction capability	a prototype based on Hyperledger Fabric	resistant to a small number of attacks
	[94]	2022	V2I	Urban	Blockchain-based authentication using fog computing over cloud computing 5G and B5G for real-time recommendations to drivers, Consensus node and fog monitor	simulations (iFogSim)	communication overhead due to interactions between fog nodes and the Cloud
	[95]	2021	V2I	–	Anonymous re-authentication based on blockchain code and transaction number for secure handover at a lower cost, RSU for authentication and blockchain consulting	analytic	storage, computational and communication cost
Intrusion detection	[57]	2022	V2V, V2I	Highway	Community revocation based on Proof of Location to prevent vehicle position-linked attacks, Traffic management centre (TMC) for Cluster processing	experiments (3 cars, 1 RSU) and simulations (SUMO, Omnet++)	detection accuracy
	[107]	2019	V2I	Highway	A Proof-of-Event consensus concept applicable to vehicular networks, The traffic data are collected through the roadside units and the passing vehicles will verify the correctness when receiving the event notification	NS-3	detection time, density impact
	[59]	2019	V2I	Urban	A message rating and credibility for trust management, RSU	simulations (SUMO, Omnet++)	computational cost, transmission overhead
	[108]	2022	V2V, V2I		A group key message rating and credibility for trust management, RSU	analytic	communication overhead, computation cost
	[104]	2020	V2V, V2I		Message and vehicle trustworthiness using trust level in blockchain, RSU for authentication and location certificate	numeric	the blocks size

Before analysing the existing works on audit in vehicular environments, it is important to define the audit, and to describe the major audit-related procedures in relation with V2X communications.

A. AUDIT DEFINITION

The origins of audit predate the Christian era, but modern auditing began in the financial field with the corporations in the early days of the Industrial Revolution. Organisations of accountants were created in the nineteens from 1853, first in the Great Britain, later in the USA and the Netherland [109]. Auditing has long been considered as an accounting procedure. It refers to the inspection and examination of companies' financial accounts to ensure that they are properly maintained in accordance with the law. Guided by the reports resulting from the audit, companies can improve risk management, control and governance.

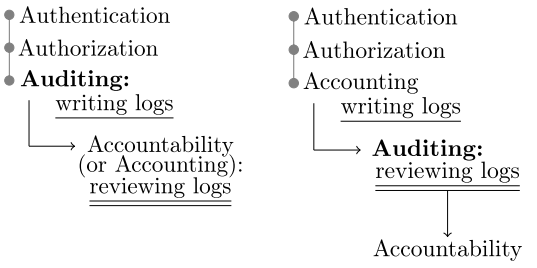
Renowned for its effectiveness, audit extends to many areas including information systems, and computer communications. Because these areas are very different from finance, there are many attempts to define auditing and adapt it to each considered area. However, even in one area, there is still no common definition of audit, neither any consensus on the steps to follow to carry it out.

In the field of information systems, where information is concerned by the audit, the first definitions date back to the 80s [110]. They focus on the organization, the mapping and the examination of the information flows throughout the different departments of a same company.

However, when it comes to modern systems in which information also flows between an organization and its external environment, information security becomes an essential part of every company needs. To be effective, security must consider several design goals, and provide a plethora of requirements/services according to the target area.

A fundamental feature of effective security is the AAA concept. The three A's in this abbreviation refer to authentication, authorization, and accounting or sometimes auditing (figure 4). Therefore, a confusion tends to arise between auditing, accounting and accountability. However, it is worth pointing out that although there are three letters in the acronym AAA, it actually involves five elements: identification, authentication, authorization, auditing and accountability. The five elements represent the security process. Here are the basic definitions of identification, authentication and authorization:

- Identification is the process of associating a representation called an identity with an entity. Any entity must present its identity when accessing a secured system.



(a) Auditing as defined in [112]

(b) Auditing as defined in [113]

FIGURE 4. Different definitions for "auditing", "accounting", and "accountability" and relatedness between concepts.

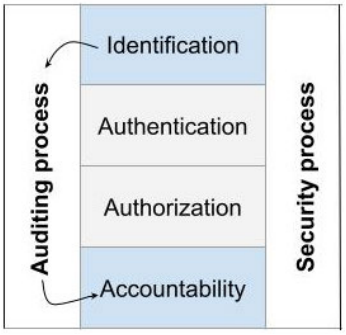


FIGURE 5. Audit process in relation with security process and features.

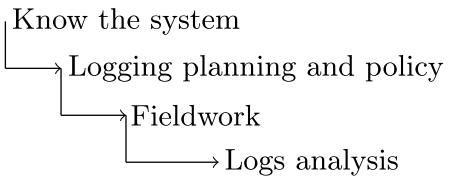


FIGURE 6. Audit phases.

- Authentication consists in proving that an entity actually has the claimed identity.
- Authorization is to define the permissions (i.e., allow/grant or deny) of accessing a resource or object for a specific identified entity.

For auditing, accounting and accountability, in order to dispel the confusion between them, many definitions have been proposed. In [111], as depicted in figure 4a, the authors suggest that "auditing" refers to "recording a log of the events and activities related to the system and subjects", while they define "accounting" and "accountability" as the processes of "reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions". In [112], as shown in figure 4b, auditing, accounting and accountability are addressed differently: auditing is "the logs review" (not accounting), accounting is "the process of writing logs of the activities of subjects and objects" (not auditing) and accountability is "the outcomes of the auditing process". Let's recall that the log file is a file which chronologically records either events occurring in an operating system or any other software running, or messages between different users of the communication system. Figures 4a and 4b show different definitions of auditing as well as its relationship with authentication and authorization, accounting and accountability.

To conclude, based on both definition attempts, apart from the conflict over naming the log file writing process either accounting or auditing, accountability - the fact of being accountable - is still carried out directly or indirectly by the auditing process, which can be seen as only writing logs or reviewing logs or both. It really depends on the target audited system and the intended objective. It may involve many investigative phases or operations and require many prior procedures. According to the ISO definition [113], an audit is "a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements, and whether these arrangements are implemented effectively and are suitable to achieve objectives". As such, in addition to being one of the security features (according to the AAA concept), auditing is a parallel process as it is managed alongside the security process and performed regularly to ensure that security is not degraded, as shown in figure 5.

B. AUDIT-RELATED PROCEDURES

The International Organization for Standardization provides guidance on managing and conducting audits. In particular, the ISO/IEC 27007[6] standard dedicated to "Information security, cybersecurity and privacy protection" gives "guidelines for information security management systems auditing". The common general phases of the auditing process, shown in figure 6, are the following:

- the "Know the system" phase is a fundamental part. Involving many steps to establish and verify the identity of the system entities, it can be seen as the identification process plus authentication. Identification process makes both traceability and accountability possible.
- the "Logging planning and policy" phase defines how and when an event has to be traced.
- the "Fieldwork" phase refers to the information collection or logging (writing logs) to obtain evidence.
- the "Logs analysis" phase represents the logging reviewing and assessment. This phase helps to identify vulnerabilities.

Regarding vehicular systems, auditing may be necessary in many cases such as accident reconstruction, attack detection, software malfunction recognition, or security maintenance. It may be thus conducted by many authorities such as a government, an insurance system, a service provider, a car manufacturer, or an application editor. In case of misbehaviour, the logs analysis aims not only at identifying malicious, but also at holding them accountable. To do this,

[6]https://www.iso.org/standard/77802.html

an identification process, which is a preliminary procedure, must be ensured. The following sections proposes a brief survey of identification and event recording in auditing systems.

1) IDENTIFICATION AND ANONYMITY

An identification system aims to assign a different identity to each singular entity (which can be a vehicle, a RSU, a pedestrian, a service, etc.) a different identity in order not to confuse them. In an ordinary road system, without a V2X communication infrastructure, vehicles are uniquely identifiable by their license plate, and potential privacy threats are confined to the geographic area of the license plate visibility [114]. It is true that the license plate is private, despite the risks of being usurped. However, the vehicle identifiers or, in general terms, the identification systems remain vital for auditing and accountability as authorities use them in their investigations to identify criminals. With the rise of V2X communications in the road network, identification procedure becomes more complex, hence identity is hardly impersonated [115]. As an example, [115] and [116] reports works and challenges using the separation of both the identifier and the location of a vehicle for scalable routing, enhancing mobility and privacy in IPv6-based vehicular networks so as to identify vehicles while protecting privacy. From a security point of view, identification is seen as a registration phase, which is the initial stage of the security process. It is usually one of the concerns of the layers above the network layer. Thus, the identifiers must identify the communicating entities independently of the way in which the messages exchanged are delivered in the network.

In [117], the authors propose a unified identification management framework and security authentication mechanism for the C-V2X equipment. An Automatic Vehicle Identification System based on RFID is proposed in [118].

The privacy concerns inherent to identification are resolved by anonymization (or anonymity) which is a common approach to protect the users' privacy, and prevent their identity disclosure. Anonymity refers to the quality of being unidentifiable, and it is mainly achieved by the means of pseudonyms [114], [119], [120]. A pseudonym is a short-term identity which replaces the long-term identifier and aims to authenticate the sender as a valid entity. They are used during the vehicular communication process as a unique identifier without any identifiable personal information.

Based on [114] - a survey of pseudonym schemes in vehicular network-, pseudonyms have a five-phase lifecycle. These phases - found in almost all pseudonym-based authentication schemes - are the following, resolution and revocation phases being optional:

- Pseudonym issuance. Most common pseudonym issuance approaches are based on third-party issuance, through which pseudonyms are created by a trusted issuing authority. This authority may have many sub-entities referred to as Certificate Authority (CA), Pseudonym Provider (PP), or Trusted Authority (TA). Other major approaches are self-issuance. In order to make sure that only valid entities can obtain pseudonyms, the pseudonym issuance phase requires that the entity owns a unique pre-installed identifier used to authenticate it. As an example, works in the scientific literature usually assumes that a connected vehicle's OBU possesses a unique vehicle digital identifier [114].
- Pseudonym use. Once the pseudonym credentials are obtained, the vehicular communication participant is able to sign outgoing messages (authentication step) as well as verify received messages (verification step).
- Pseudonym change. The main motivation for pseudonyms is the protection of identity, and therefore the preservation of privacy. In order to prevent tracking attacks, pseudonyms have a short-term validity, as do all entity-related identifiers to the application, protocol, and network layers. The desired level of privacy determines the frequency of pseudonyms change. In order to enable an effective anonymity context, multiple neighbouring entities are required to simultaneously change their pseudonyms. A great deal of research on pseudonym change strategies has been carried out in the last decade, some of which are described in [121].
- Pseudonym resolution. This phase concerns in particular the law enforcement representatives in particular when holding misbehaviour accountability. To obtain the long-term identity of an entity from its pseudonyms, a resolution request should be addressed to the issuing authority or the pseudonyms provider which verifies the eligibility of the request.
- Pseudonym revocation. Nodes which are judged as being faulty should be revoked from the network in order to preserve a proper functioning of the latter. This may entail the revocation of the credentials, including the long-term identity.

2) EVENT RECORDING

To maintain the security of both vehicle communications and on-board software, auditing is a proven security best practice. As mentioned above, the audit process requires the identification of entities and the recording of communications and events in log files/audit trails, which are fundamental features of the audit process to ensure accountability. Many physical sites exist to store audit trails: in vehicles (using an Event Data Recorder (EDR)/''black box'') or externally (e.g. cloud storage). A comparative study between both sites is presented in Table 5.

The major issue with data storage sites is data integrity. Usually, with EDRs, the problem is dealt with physically [122]. They are mainly protected against unauthorized access and physical damage, ditto for cloud storage. However, as an internet-connected technology, cloud storage is most exposed to increased attacks [113]. Additionally, in some cases, data outsourced to cloud storage can no longer be controlled by data owners/vehicles. Therefore, data integrity

TABLE 5. A comparative summary of log files storage sites.

	in-vehicle e.g.: EDR/"black box"	outside the vehicle e.g.: cloud storage
Security	mainly secured against unauthorized access, physical damage and tampering via integrity protection using checksum	prone to forgery attacks; data deletion; data are no longer possessed by vehicles
Size	cannot be unlimited	unlimited
Data transfer medium	Controller Area Network buses	Mobile Wireless technologies
Data source	sensors	vehicle wireless interfaces
Common problem	data might be corrupted during transmission	

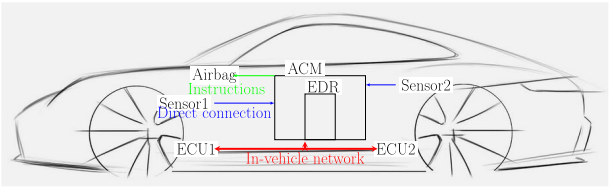


FIGURE 7. EDR data collection and interconnection with in-vehicle sensors (inspired from [123]).

auditing becomes necessary to ensure the integrity of stored data.

Following this track, we have classified the existing audit-related solutions into two categories: i) EDR/"black box" category in which the proposals relate more to the technical design of such equipment used to record data for accident reconstruction, and ii) Cloud data storage audit category in which proposals improve data integrity in the Cloud to prohibit tampering with outsourced data. To strengthen the integrity, the traceability and the possibility of designing distributed audit trails, some solutions belonging to both categories used the blockchain technology.

EDR/black box

Like the aircraft flight data recorder, EDR, as illustrated in figure 7, captures and stores vehicle data for several seconds before, during and after any crash where an airbag is triggered or there is an excessive rate of vehicle deceleration [123], [124]. Nowadays, innovative EDR records various types of data - which comes from different mounted sensors - used to diagnose a wide range of car problems which can cause accidents resulting in lawsuits and insurance claims [124].

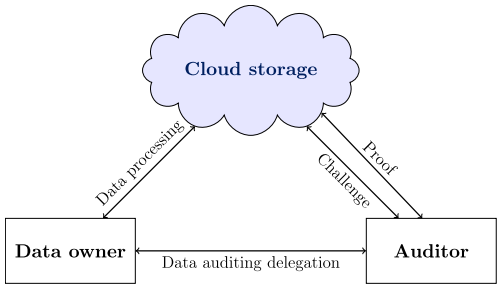


FIGURE 8. The system model of the data integrity auditing (inspired from [128]).

EDR data can also help with location tracking when the car is stolen or lost. In short, EDR is becoming a powerful tool in vehicles, helping to make transportation safer and more responsible [125].

The authors of [123] surveyed and performed experiments on real EDRs, and they verified that information related to evidence of hacking can be obtained in addition to conventional information about an accident in the traffic.

The work in [126] presents a method to synchronize data acquisition devices which are mechanically coupled, by the means of an accelerometer attached to each device.

In [127], a distributed and stratified "black box" audit trail for automotive software and data provenance is proposed to assure users, service providers, and original equipment manufacturers (OEMs) of vehicular software integrity and reliability. The proposed black box architecture is both layered and broadcasted, employing distributed hash tables (DHT), a parity system and a public blockchain to provide high resilience, assurance, scalability, and efficiency for automotive and other safety-sensitive systems.

Finally, [122] presents a distributed, blockchain-based juridical recording unit ZugChain which opportunistically utilizes on-train hardware. ZugChain offers high reliability via replication and tamper-resistance due to the nature of blockchains. It implements a permissioned blockchain based on a Byzantine fault-tolerant agreement protocol suitable for diverse communication systems. To utilize the logged data for advanced services, e.g. predictive maintenance, ZugChain securely and continuously exports traces to private data centres.

Auditing cloud data storage

In literature, most researchers are concerned about the integrity of outsourced data and data transferred to the cloud. In fact, storage is one the services provided by cloud computing. Because of the limited resources of the vehicles, the cloud could allocate computing or storage resources to authorized vehicles to communicate or share information with each other and with service providers. This implies that the vehicles lose the control of their data. As cloud resources can be subject to security risks, data may be damaged or deleted [128], [129], [130]. Auditing in this case consists in performing the necessary procedures to ensure and verify

data integrity. To do so, the authors of [128] and [129] model the system in three parts as shown in figure 8: the owners of data, also called tenants, which create and share their data, the cloud server which stores that data, and the third-party auditor, which provides data integrity auditing services.

Reference [128] proposes a dynamic data integrity auditing scheme supporting data privacy protection. First, the authors build a hierarchical multiple branches tree data authentication structure in the initialization phase. Then, they design a data integrity auditing scheme based on the bilinear pairing mapping technology and the Boneh-Lynn-Shacham digital signature mechanism.

A new shared data auditing scheme is proposed in [129], which supports user' revocation by combining an existing certificateless signcryption method with a fog architecture. This scheme improves the efficiency of auditing and user revocation, since it reduces many time-consuming operations, as well as achieves features such as public auditing, mutual authentication, and both efficient and secure revocation.

A different approach for cloud data integrity auditing was proposed in [130]. Authors propose an offline data integrity verification using blockchain. Featured with tamper-proofing, blockchain is integrated in the cloud auditing system, thus allowing to reduce the communication cost between the auditor and the cloud data. Inspired by the data structure of blockchain, the authors of [130] design an evidence chain to achieve offline auditing, which allows the Cloud to spontaneously generate data integrity evidence without communicating with auditors during the evidence generation phase. Furthermore, they extend their scheme to support public and automatic validation based on smart contracts.

To summarize, the majority of existing auditing schemes have been proposed in order to ensure the integrity of data in the Cloud. They are summarized in Table 6.

V. PERSPECTIVE ON V2X COMMUNICATIONS AUDIT

Most of the works reviewed in this survey may contribute to Vehicle-to-everything communications audit. However, they need to be put into a framework which will offer a global approach to V2X communications audit covering the diversity of vehicle operating environments. Indeed, though the contemporary security approaches, including those based on the blockchain, can apply straightforwardly to the context of Vehicle-to-infrastructure communications, it is necessary to investigate the potentiality of their effective application to vehicle ad hoc communications as well. Referring to figure 9, this section explores the different issues which should be tackled in future works regarding different aspects.

A. THE CONFLICT BETWEEN PRIVACY AND AUDITING

Vehicles evolve in a public space while in the road traffic. Therefore, maintaining the privacy of information of their owners during the auditing procedure is a critical subject. On one side, the audit procedure requires the access and the analysis of the entire system data. On the other side, the audited data can contain private and sensitive information. To overcome the problem, the establishment of conditional anonymity seems essential to the proper functioning of the audit procedure in case of misbehaviour [134]. In pseudonymous authentication schemes, auditability can be supported by enabling the conditional anonymity. In this case, users' identity remains anonymous unless they misbehave. Also, the ability to trace a pseudonym to the pseudonym holder's identity is restricted to specific authorities (auditors). Only privileged and trustful auditor can trace, or resolve, a pseudonym to an identity, under specific conditions.

Furthermore, one of the privacy related features which complicate the auditing are pseudonyms' change and revocation. Even with the conditional anonymity, mapping the pseudonym to the original identity is sometimes difficult [57]. In fact, pseudonyms are designed to avoid tracking. That is why each entity, in particular a vehicle, can obtain a large number of temporary pseudonyms, which are frequently alternated or changed along its trajectory. It is worth emphasizing that many authorities may be involved in the management of pseudonyms [121]. Making the mapping possible requires that all the pseudonym's operations of each entity within each authority are logged. Though this can be achieved easily in the context of V2I communications (left part of figure 9), it is necessary to explore and consolidate efficient identification and pseudonyms for vehicles in the context of vehicular ad hoc networks where no infrastructure is accessible. An early work [135] attempted to propose a framework for authentication through certificates, privacy through pseudonyms, and auditability of the communications. However, the latter remained dependent on infrastructure access points. There is still a need for fully distributed audit in a context where only vehicle-to-vehicle communications are possible (right part of figure 9).

B. AUDIT ACCEPTABILITY

Due to its open and ephemeral nature, V2X network is highly vulnerable to attacks. A wealth of work on V2X security has been published to detect and mitigate security breaches which can result from misbehaviour or software or hardware malfunction. Undetected ones are handled through the audit procedure.

Due to continuous technological development, advances are occurring on both sides: security defences as well as attack techniques. As such, auditing becomes a must to maintain the level of security as well as to anticipate potential future dangers. In fact, the auditing procedure includes a monitoring process where all system events are recorded in audit trails/logs. In addition, the audit includes an analysis process during which the audit trails/logs are thoroughly

TABLE 6. EDR and Cloud audit works.

	Ref	Year	Contribution	Advantages
Event data recorder (EDR)	[131]	2019	An analysis of many EDR data elements specificity and sensitivity.	To meet different applications needs
	[124]	2021	An android application, connected to a set of sensors, used to transmit signals or a call to the closest ambulance, police departments, and trustworthy friends and family members in case of accident.	Light and easy application to use enhancing legacy EDRs performance and cost although they use limited storage SD card
	[132]	2022	An integrated system which frequently monitors the parameters of moving cars using mounted sensors.	Real-time warning for the driver, plus extended data storage systems
	[133]	2022	A data-driven model used to compress and identify key events which should be conserved in the EDR subsystem.	Useful for resource constrained autonomous vehicles.
	[122]	2022	A blockchain-based event recorder for railway systems.	High reliable event recording via replication and tamper-resistance due to the nature of blockchain.
Cloud audit	[128]	2018	A Hierarchical Multiple Branches Tree (HMBT) for data authentication structure in the initialization phase and a data integrity auditing scheme based on the bilinear pairing mapping technology.	Resists forgery attack and replay attack, protects data privacy and assures public auditing
	[129]	2020	A fog-assisted shared data auditing scheme supporting users' revocation process	Reduces time-consuming operations and allows public auditing, mutual authentication, efficient and secure revocation

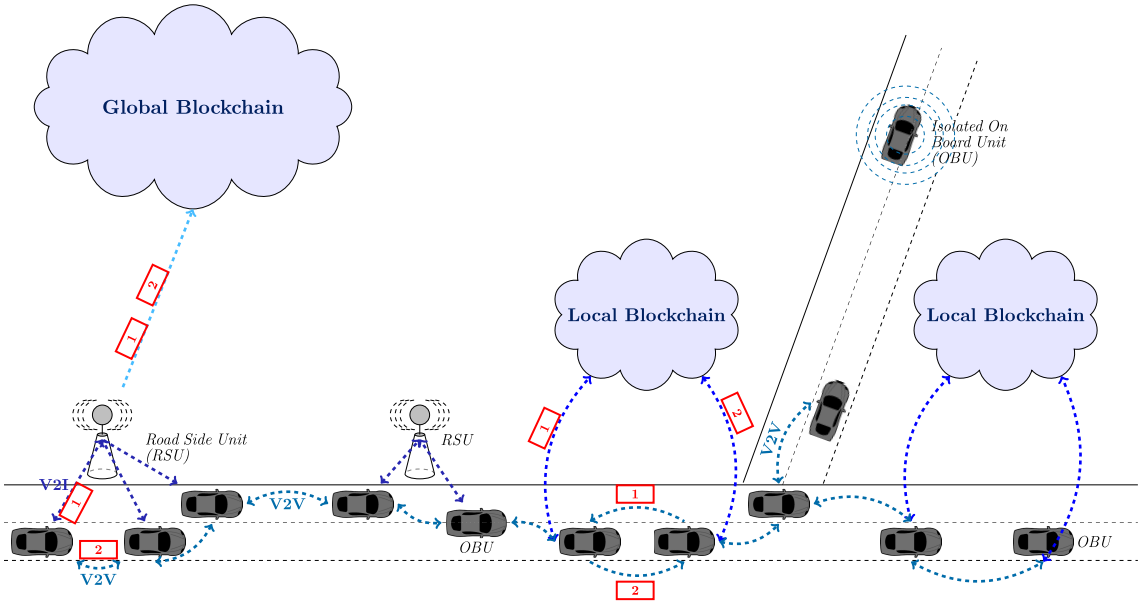


FIGURE 9. Local and global blockchains.

reviewed to verify compliance of system components and compliance with laws and standards requiring privacy, integrity, availability, confidentiality and authentication protection.

However, audit trails are considered as a double-edged sword. As they serve to provide security, they can also be seen as unacceptable records of users' private data [136]. Thus, audit can be at the origin of a societal debate since the users participating in cooperative applications in the road traffic through their car refuse consent the traceability, recording and potentially exposure of their activity to attackers' attempts against them. Therefore, auditing needs to be carefully addressed by designing a data-privacy friendly audit process, justified as a mean for justice to operate through autho-

rized authorities when forfeitures are committed through V2X communications, which the public will accept more easily.

C. DATA STORAGE AND INTEGRITY

Vehicular communications tracing will generate a massive amount of heterogeneous data. Storing these data for auditing purposes represents a great challenge. A substantial solution to increase storage capacity and data consistency is Cloud storage which can store a large amount of data in a flexible way and at lower costs [137].

However, despite all related advantages, Cloud services can be subject to major security issues which draw the attention of many researchers [138], [139]. As such, Cloud security is among the concerns which require attention when designing Cloud-based audit trail storage.

Moreover, it would be questionable to consider that every communication traces should be stored for audit purposes even when no notable event has occurred. An efficient auditing system should define some criteria both for the data which need to be stored, and the duration of their conservation. This is particularly important in the context of V2V communications where the infrastructure is inaccessible in order to send the data to the Cloud, and where the vehicles are obliged to use their local storage for audit data.

Finally, due to the dynamic of vehicles in the road traffic, several records related to the same event may come from the same location area and at the same time from many different vehicles. It is necessary to include data fusion mechanisms and a storage policy which will tackle this problem efficiently in the design of an auditing system.

D. DYNAMIC TOPOLOGY

Dynamic topology is inherent to vehicular networks. Vehicles can move in several different environments, which influences both their speed, neighbourhood and data needs. It is not guaranteed for vehicles to be connected with the same neighbour vehicles, RSUs or Cloud servers all along their ride time. Disconnection or isolation can occur frequently (upper-right part of figure 9). Relying on Cloud storage and services seems insufficient to keep the traces of all exchanged data and guarantee audit. An effective audit system should take into account all the features and advances of the vehicle system which can be advantageous to enable new functionalities and anticipate failures. One of the most promising research trends for providing continuous transmission coverage and always-on connectivity is the new dynamic RSU deployment patterns. Based on vehicle mobility, the dynamic RSU can be vehicles, parked cars, bus lines or Unmanned Aerial Vehicles (UAVs), which contribute to maintain connectivity as much as possible, and thus promote the Internet of Vehicles (IoV) [140]. Nevertheless, the comparative study in [140] confirms that the performance of the different RSU placement solutions strongly depends on several factors such as the shape of the road, the particularity of the road segments (such as those prone to accidents), the wireless access methods, the mobility pattern, and the distribution of vehicles in time and space. Therefore, keeping the audit log will heavily depend on these factors. Alternatively, V2X communications include the V2V communication mode which supports mobility and may compensate the absence of RSU for local communications between vehicles. Indeed, by reducing the system dependence on the infrastructure, V2V communications improve autonomy and play a key role in cooperative applications such as collaborative perception which is essential to Intelligent Transport Systems (ITS) [141], [142]. However, it is not easy to define how audit data collection and storage could be performed in this context in a way that keeps them trustworthy for future investigations.

E. BLOCKCHAIN BASED SOLUTIONS FOR AUDIT

The decentralization, traceability and tamper resistance are among the major enablers of successful audit. Blockchain technology ensures these features efficiently and provides others which can be beneficial for effective auditing. Using blockchain, vehicular communications can be stored in a transparent and decentralized way as transactions. Along with all the benefits offered by blockchain, there are many issues encountered when implementing a blockchain based solution in the context of vehicular communications. Originally, blockchains were designed for relatively small monetary transactions [143]. When it comes to vehicular environment, the events can correspond to message generation. Assuming that each transaction will include a timestamp, the sender and recipient addresses, and probably the message type and content, and every necessary data for auditing. Using an ITS G5 communication system, the size of periodic status information such as CAM (Context Aware Message) is between 200 bytes and 800 bytes, and it is broadcasted every 0.1 seconds [57] by all connected vehicles. As such, the massive data generated result in mega blocks which cannot be handled by traditional blockchain. Furthermore, over time, the size of the blockchain itself gets bigger and bigger. Not only the storage of the blockchain is problematic, but also the high computing become challenging. Processing of large blocks by all nodes becomes a problem as it increases the blockchain throughput (the number of transactions validated per second).

In an infrastructure environment, resorting to Cloud solutions could help creating and managing the blockchain, which may solve both the processing and the storage problems. However, in a context where only V2V communications are possible, there is no access to the Cloud. Therefore, blockchain creation and management should be achieved distributively by the vehicles. This raises new issues such as:

- which vehicle can create a new blockchain?
- how should be formed the group of vehicles participating to the same blockchain?
- how the decision of keeping or archiving a running Blockchain should be taken according to the changes in the participating nodes?

- how the different Blockchains archived in that infrastructureless context should be merged by the infrastructure servers when the vehicles come back in covered areas?

In addition, in a blockchain network, every nodes are able to check the transactions. This mcompromises both confidentiality and privacy of data for transparency reasons. This problem joins the privacy issue posed by the auditing process. Several recent work address confidentiality preserving in Blockchain, using classical cryptography solutions [144], or innovative one such as zero-knowledge proof [145]. Such approaches should be investigated in the context of Blockchain-based vehicular network audit.

F. LACK OF STANDARDS

The audit process is not just an after-the-fact verification. It involves many operations and has a set of important features. It depends on the application's nature and requirements as well as the country. A successful audit process starts as soon as the system/application is deployed. To design applications which support auditability, a number of conditions, policies, requirements and stages must be defined beforehand. The initiatives of car manufacturers in this context are reflected by the fact of equipping vehicles with black boxes considered as one of the new mandatory safety features hailed by the European Commission [146]. ETSI recommends keeping an audit log of the type and content of each message sent and received by a communicating entity [147]. However, to our knowledge, there is no ETSI document which standardizes the audit in V2X communications, especially in the context of vehicle-to-vehicle communication only. The standards can provide guidance and recommendations for the future audit specifications and then facilitate the audit establishment. The lack of standards defining auditing can sow confusion between accountability and auditing in both the academic and industrial fields. Fortunately, the lack of standards makes room for new ideas and opens up new horizons for innovation in auditing in V2X.

VI. CONCLUSION

Vehicular systems are continuously evolving, promoting vehicle autonomy and smartness, which aim at providing safer future roads and smoother driving. As vehicular systems become more open and technologically more complex, vehicles become more vulnerable to attacks on security and privacy, especially in cooperative applications. Many proactive and reactive security approaches have been proposed. However, a few studies have focused on auditing, one of the basic security tools, which is essential for both reporting security vulnerabilities and identifying deviant acts and actors involved in accident construction. In this article, we have reported identification methods and pseudonymization mechanisms in vehicular environments. We have also covered the most relevant work in relation to the auditing process and tools in the context of vehicular communications. In particular, we have presented a study of the existing solutions to event recording in the vehicle's system, and discussed the use of Blockchain technology as a potential solution. Finally, we have pointed out the challenges that such solutions should address in order to offer efficient auditing in vehicular communications, especially when only vehicle-to-vehicle communications are possible.

REFERENCES

[1] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, Aug. 2020.

[2] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A survey," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107093.

[3] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100164.

[4] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," *IEEE Trans. Intell. Vehicles*, vol. 5, no. 4, pp. 693–713, Dec. 2020.

[5] B. Khalfoun, M. Maouche, S. Ben Mokhtar, and S. Bouchenak, "MooD: Mobility data privacy as orphan disease: Experimentation and deployment paper," in *Proc. 20th Int. Middleware Conf.*, Dec. 2019, pp. 136–148.

[6] A. Quyoom, A. A. Mir, and D. A. Sarwar, "Security attacks and challenges of VANETs : A literature survey," *J. Multimedia Inf. Syst.*, vol. 7, no. 1, pp. 45–54, Mar. 2020.

[7] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101664.

[8] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 2, pp. 760–776, Feb. 2019.

[9] Z. Sun, Y. Li, and W. Zhang, "Research on the development trend and auditing mode of high security enterprise intranet security audit," in *Proc. IEEE 11th Int. Conf. Adv. Infocomm Technol. (ICAIT)*, Oct. 2019, pp. 153–156.

[10] G. Costantino, F. Martinelli, and I. Matteucci, "Reputation systems to mitigate DoS attack in vehicular network," in *Critical Information Infrastructures Security* (Lecture Notes in Computer Science), vol. 10707, G. D'Agostino and A. Scala, Eds. Cham, Switzerland: Springer, 2017.

[11] G. Primiero, A. Martorana, and J. Tagliabue, "Simulation of a trust and reputation based mitigation protocol for a black hole style attack on VANETs," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Apr. 2018, pp. 127–135.

[12] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 996–1014, Mar. 2018.

[13] J. Grover, "Security of vehicular ad hoc networks using blockchain: A comprehensive review," *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100458.

[14] X. Wang, C. Xu, Z. Zhou, S. Yang, and L. Sun, "A survey of blockchain-based cybersecurity for vehicular networks," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 740–745.

[15] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1212–1239, 4th Quart., 2022.

[16] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[17] P. Saraswathi, G. Rajkumar, and P. M. Rao, "Intelligent transport system using IoT-V2X: Communication technologies, security issues, challenges and countermeasures," *Res. Square*, 2022.

[18] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang, and S. Yu, "Attacks and defences on intelligent connected vehicles: A survey," *Digit. Commun. Netw.*, vol. 6, no. 4, pp. 399–421, Nov. 2020.

[19] R. W. van der Heijden, S. Dietzel, T. Leinmüller, and F. Kargl, "Survey on misbehavior detection in cooperative intelligent transportation systems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 779–811, 1st Quart., 2019.

[20] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," *IEEE Access*, vol. 9, pp. 162401–162437, 2021.
[21] D. K. Hassan Farran and L. Bokor, "A comprehensive survey on the application of blockchain/hash chain technologies in V2X communications," *Infocommunications J.*, vol. 14, no. 1, pp. 24–35, 2022.
[22] R. Kumar and J. Singh, "Internet of Vehicles (IOV) over VANETs: Smart and secure communication using IoT," *Scalable Comput., Pract. Exper.*, vol. 21, no. 3, pp. 425–439, 2020.
[23] R. Gasmi and M. Aliouat, "Vehicular ad hoc networks versus Internet of Vehicles—A comparative view," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, Jun. 2019, pp. 1–6.
[24] A. Zekri and W. Jia, "Heterogeneous vehicular communications: A comprehensive study," *Ad Hoc Netw.*, vols. 75–76, pp. 52–79, Jun. 2018.
[25] M. Khabbaz, C. Assi, and S. Sharafeddine, "Multihop V2U path availability analysis in UAV-assisted vehicular networks," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10745–10754, Jul. 2021.
[26] B. Manale and T. Mazri, "5G, vehicle to everything communication: Opportunities, constraints and future directions," *Adv. Sci., Technol. Eng. Syst. J.*, vol. 5, no. 6, pp. 1089–1095, 2020.
[27] M. Fowler, T. Geiselbrecht, R. Brydia, G. Geary, and M. Manser, "Addressing the motorcyclist advisory council recommendations: Synthesis on intelligent transportation system applications and automated technologies for motorcyclists," Performing organisation: Texas A&M Transportation Institute; Sponsoring Agency: U.S. Department of Transportation, Federal Highway Administration, Office of Safety, Washington, DC, USA, Tech. Rep. FHWA-SA-22-033, 2022.
[28] A. A. Khan, V. Kumar, M. Ahmad, and S. Jangirala, "A secure and energy efficient key agreement framework for vehicle-grid system," *J. Inf. Secur. Appl.*, vol. 68, Aug. 2022, Art. no. 103231.
[29] N. Chen, M. Wang, N. Zhang, and X. Shen, "Energy and information management of electric vehicular network: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 967–997, 2nd Quart., 2020.
[30] J. Huang, M. Zhao, Y. Zhou, and C.-C. Xing, "In-vehicle networking: Protocols, challenges, and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 92–98, Jan. 2019.
[31] T. Chatterjee, R. Karmakar, G. Kaddoum, S. Chattopadhyay, and S. Chakraborty, "A survey of VANET/V2X routing from the perspective of non-learning- and learning-based approaches," *IEEE Access*, vol. 10, pp. 23022–23050, 2022.
[32] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in *Ad Hoc Networks* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 49, J. Zheng, D. Simplot-Ryl, V. C. M. Leung, Eds. Berlin, Germany: Springer, 2010.
[33] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100310, doi: 10.1016/j.vehcom.2020.100310.
[34] S. Patrick, R. Lucas, and W. Martine, "Supporting multiple cooperative applications through vehicle-to-vehicle communications," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Dec. 2019, pp. 1–6.
[35] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-vehicle communication in C-ACC/platooning scenarios," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 192–197, Aug. 2015.
[36] N. Cenerario, T. Delot, and S. Ilarri, "A content-based dissemination protocol for VANETs: Exploiting the encounter probability," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 771–782, Sep. 2011.
[37] G. Xiog, T. Yang, M. Li, Y. Zhang, W. Song, and J. Gong, "A novel V2X-based pedestrian collision avoidance system and the effects analysis of communication delay and packet loss on its application," in *Proc. IEEE Int. Conf. Veh. Electron. Saf. (ICVES)*, 2018, pp. 1–6.
[38] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, "Enhancements of V2X communication in support of cooperative autonomous driving," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 64–70, Dec. 2015.
[39] Y. H. Kwon, "Improving multi-channel wave-based V2X communication to support advanced driver assistance system (ADAS)," *Int. J. Automot. Technol.*, vol. 17, no. 6, pp. 1113–1120, Dec. 2016.
[40] B. L. Nguyen, D. T. Ngo, and H. L. Vu, *Vehicle Communications for Infotainment Applications*. Singapore: Springer, 2022, pp. 705–722, doi: 10.1007/978-981-287-251-7_44.
[41] *5G Americas White Paper: Cellular V2X Communications Towards 5G*, Bellevue, WA, USA, Mar. 2018.
[42] *Report ITU-R M.2445-0 (11/2018)—Intelligent Transport Systems (ITS) Usage*, ITU-R, Geneva, Switzerland, 2018.
[43] K. Sehla, T. M. T. Nguyen, G. Pujolle, and P. B. Velloso, "Resource allocation modes in C-V2X: From LTE-V2X to 5G-V2X," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8291–8314, Jun. 2022.
[44] 5G Americas Whitepaper. (Mar. 2018). *Cellular V2X Communications Towards 5G*. Accessed: Mar. 20, 2023. [Online]. Available: https://www.5gamericas.org/white-papers/
[45] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Standard 802.11p-2010, pp. 1–51, 2010.
[46] V. Mannoni, V. Berg, S. Sesia, and E. Perraud, "A comparison of the V2X communication systems: ITS-G5 and C-V2X," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5.
[47] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 4, pp. 504–518, 2nd Quart., 2010.
[48] *IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture*, IEEE Standard 1609.0-2019, pp. 1–106, 2019.
[49] G. Naik, B. Choudhury, and J.-M. Park, "IEEE 802.11bd & 5G NR V2X: Evolution of radio access technologies for V2X communications," *IEEE Access*, vol. 7, pp. 70169–70184, 2019.
[50] M. H. C. Garcia, A. Molina-Galan, M. Boban, J. Gozalvez, B. Coll-Perales, T. Sahin, and A. Kousaridas, "A tutorial on 5G NR V2X communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1972–2026, 3rd Quart., 2021.
[51] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
[52] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, ETSI EN 302 637-2 V1.4.1 (2019-04), 2019.
[53] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, ETSI EN 302 637-3 V1.3.1 (2019-04), 2019.
[54] *NetSim Applications Unmanned Aerial Vehicle (UAV) Communication*. Accessed: Jul. 1. [Online]. Available: https://www.tetcos.com/
[55] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102779.
[56] C. Sommer, D. Eckhoff, A. Brummer, D. S. Buse, F. Hagenauer, S. Joerer, and M. Segata, "Veins: The open source vehicular network simulation framework," in *Recent Advances in Network Simulation*. Cham, Switzerland: Springer, 2019.
[57] A. Didouh, H. Labiod, Y. E. Hillali, and A. Rivenq, "Blockchain-based collaborative certificate revocation systems using clustering," *IEEE Access*, vol. 10, pp. 51487–51500, 2022.
[58] M. Awais Hassan, U. Habiba, U. Ghani, and M. Shoaib, "A secure message-passing framework for inter-vehicular communication using blockchain," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 2, Feb. 2019, Art. no. 155014771982967.
[59] A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors*, vol. 19, no. 22, p. 4954, Nov. 2019.
[60] B. Schünemann, "V2X simulation runtime infrastructure VSimRTI: An assessment tool to design smart traffic management systems," *Comput. Netw.*, vol. 55, no. 14, pp. 3189–3198, Oct. 2011.
[61] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, no. 2, p. 334, Jan. 2019.
[62] J. S. Weber, M. Neves, and T. Ferreto, "VANET simulators: An updated review," *J. Brazilian Comput. Soc.*, vol. 27, no. 1, pp. 1–12, Dec. 2021.
[63] K. G. Lim, C. H. Lee, R. K. Y. Chin, K. Beng Yeo, and K. T. K. Teo, "SUMO enhancement for vehicular ad hoc network (VANET) simulation," in *Proc. IEEE 2nd Int. Conf. Autom. Control Intell. Syst. (I2CACIS)*, Oct. 2017, pp. 86–91.
[64] M. Fellendorf and P. Vortisch, "Microscopic traffic flow simulator VISSIM," in *Fundamentals of Traffic Simulation* (International Series in Operations Research & Management Science), vol. 145, J. Barceló, Eds. New York, NY, USA: Springer, 2010.
[65] C. L. Azevedo, N. M. Deshmukh, B. Marimuthu, S. Oh, K. Marczuk, H. Soh, K. Basak, T. Toledo, L.-S. Peh, and M. E. Ben-Akiva, "SimMobility short-term: An integrated microscopic mobility simulator," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2622, no. 1, pp. 13–23, Jan. 2017.

[66] G. D. B. Cameron and G. I. D. Duncan, "PARAMICS? Parallel microscopic simulation of road traffic," *J. Supercomput.*, vol. 10, no. 1, pp. 25–53, 1996.

[67] W. S. Halati and H. Lieu, "Corsim-corridor traffic simulation model," in *Proc. Traffic Congestion Traffic Saf. 21st Century, Challenges, Innov., Opportunities*, 1997, pp. 1–20.

[68] A. Varga, "OMNeT++," in *Modeling and Tools for Network Simulation*, K. Wehrle, M. Güneş, and J. Gross, Eds. Berlin, Germany: Springer, 2010.

[69] OPNET Projects team. *OPNET—Optimun Network Performance*. Accessed: Jul. 1. [Online]. Available: https://opnetprojects.com/

[70] R. Barr, Z. Haas, and R. V. Renesse. *JIST/SWANS: Java in Simulation Time/Scalable Wireless Ad Hoc Network Simulator*. Accessed: Jul. 1. [Online]. Available: http://jist.ece.cornell.edu/

[71] G. Carneiro, "NS-3: Network simulator 3," in *Proc. UTM Lab Meeting*, 2010, pp. 4–5.

[72] T. Issariyakul and E. Hossain, "Introduction to network simulator 2 (NS2)," in *Introduction to Network Simulator NS2*. Boston, MA, USA: Springer, 2010.

[73] P. Sondi, I. Abbassi, E. Ramat, E. Chebbi, and M. Graiet, "Modeling and verifying clustering properties in a vehicular ad hoc network protocol with event-B," *Sci. Rep.*, vol. 11, no. 1, p. 17620, Sep. 2021.

[74] N. Benaissa and D. Méry, "Cryptographic protocols analysis in event B," in *Perspectives of Systems Informatics*, A. Pnueli, I. Virbitskaite, and A. Voronkov, Eds. Berlin, Germany: Springer, 2010, pp. 282–293.

[75] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso, and J. Alonso-Zarate, "A comprehensive survey of V2X cybersecurity mechanisms and future research paths," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 325–391, 2023.

[76] A. Verma, R. Saha, G. Kumar, and T.-H. Kim, "The security perspectives of vehicular networks: A taxonomical analysis of attacks and solutions," *Appl. Sci.*, vol. 11, no. 10, p. 4682, May 2021.

[77] P. S. Kumar, L. Parthiban, and V. Jegatheeswari, "Context aware privacy and security using P-gene based on pseudonym in VANETs," in *Proc. IEEE Int. Conf. Intell. Techn. Control, Optim. Signal Process. (INCOS)*, Jan. 2019, pp. 1–5.

[78] M. B. Mansour, C. Salama, H. K. Mohamed, and S. A. Hammad, "VANET security and privacy—An overview," *Int. J. Netw. Secur. Appl.*, vol. 10, no. 2, pp. 13–34, Mar. 2018.

[79] L. Benarous and B. Kadri, "Privacy preserving scheme for pseudonym refilling in VANET," in *Proc. Int. Conf. Smart Commun. Netw. Technol. (SaCoNeT)*, Oct. 2018, pp. 114–119.

[80] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021.

[81] C. Huang, "Effective privacy-preserving mechanisms for vehicle-to-everything services," Ph.D. dissertation, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, 2020. [Online]. Available: http://hdl.handle.net/10012/16181

[82] J. Huang, D. Fang, Y. Qian, and R. Q. Hu, "Recent advances and challenges in security and privacy for V2X communications," *IEEE Open J. Veh. Technol.*, vol. 1, pp. 244–266, 2020.

[83] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, 4th Quart., 2011.

[84] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in V2X communication systems," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1–36, Sep. 2023.

[85] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," Tech. Univ. Dresden, Dresden, Germany, Tech. Rep. 10.1.1.154.635, pp. 1–98, 2010.

[86] I. Ivanov, C. Maple, T. Watson, and S. Lee, "Cyber security standards and issues in V2X communications for Internet of Vehicles," in *Living in the Internet of Things: Cybersecurity of the IoT*. London, U.K., 2018, pp. 1–6.

[87] W. Hathal, H. Cruickshank, Z. Sun, and C. Maple, "Certificateless and lightweight authentication scheme for vehicular communication networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16110–16125, Dec. 2020.

[88] S. Bittl, K. Roscher, and A. A. Gonzalez, "Security overhead and its impact in VANETs," in *Proc. 8th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Oct. 2015, pp. 192–199.

[89] P. Cincilla, O. Hicham, and B. Charles, "Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–8.

[90] F. Haidar, A. Kaiser, and B. Lonc, "On the performance evaluation of vehicular PKI protocol for V2X communications security," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2017, pp. 1–5.

[91] I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A blockchain approach for decentralized V2X (D-V2X)," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4001–4010, May 2021.

[92] Y. Zhang, F. Tong, Y. Xu, J. Tao, and G. Cheng, "A privacy-preserving authentication scheme for VANETs based on consortium blockchain," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, Nov. 2020, pp. 1–6.

[93] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "HyperLedger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[94] T. Baker, M. Asim, H. Samwini, N. Shamim, M. M. Alani, and R. Buyya, "A blockchain-based fog-oriented lightweight framework for smart public vehicular transportation systems," *Comput. Netw.*, vol. 203, Feb. 2022, Art. no. 108676.

[95] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: Blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, Feb. 2021.

[96] J. Su, R. Ren, Y. Li, R. Y. K. Lau, and Y. Shi, "Trusted blockchain-based signcryption protocol and data management for authentication and authorization in VANETs," *Wireless Commun. Mobile Comput.*, vol. 2022, pp. 1–14, May 2022.

[97] S. Aggarwal, N. Kumar, and P. Gope, "An efficient blockchain-based authentication scheme for energy-trading in V2G networks," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6971–6980, Oct. 2021.

[98] Y. Tan, J. Wang, J. Liu, and N. Kato, "Blockchain-assisted distributed and lightweight authentication service for industrial unmanned aerial vehicles," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 16928–16940, Sep. 2022.

[99] M. Shen, H. Lu, F. Wang, H. Liu, and L. Zhu, "Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12250–12263, Nov. 2022.

[100] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021.

[101] A. Alnasser, H. Sun, and J. Jiang, "Cyber security challenges and solutions for V2X communications: A survey," *Comput. Netw.*, vol. 151, pp. 52–67, Mar. 2019.

[102] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21266–21289, 2019.

[103] M. Firdaus and K.-H. Rhee, "On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks," *Appl. Sci.*, vol. 11, no. 1, p. 414, Jan. 2021.

[104] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, May 2020.

[105] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[106] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5G-enabled vehicular networks," *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020.

[107] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[108] X. Li and X. Yin, "Blockchain-based group key agreement protocol for vehicular ad hoc networks," *Comput. Commun.*, vol. 183, pp. 107–120, Jan. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421004588

[109] R. Hayes, P. Wallage, and H. Gortemaker, *Principles of Auditing: An Introduction to International Standards on Auditing*. London, U.K.: Pearson, 2014.

[110] H. Vo-Tran, "Adding action to the information audit," *Electron. J. Inf. Syst. Eval.*, vol. 14, pp. 271–281, Jan. 2011.

[111] M. Chapple, J. M. Stewart, and D. Gibson, *(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide*. Alameda, CA, USA: Sybex, 2021.
[112] W. Wu, *The Effective CISSP: Security and Risk Management* (The Effective CISSP). Taiwan: Wentz Wu, 2020.
[113] L. M. Bruma, "Cloud security audit—Issues and challenges," in *Proc. 16th Int. Conf. Comput. Sci. Educ. (ICCSE)*, Aug. 2021, pp. 263–266.
[114] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.
[115] J. Jeong, Y. Shen, T. Oh, S. Céspedes, N. Benamar, M. Wetterwald, and J. Härri, "A comprehensive survey on vehicular networks for smart roads: A focus on IP-based approaches," *Veh. Commun.*, vol. 29, Jun. 2021, Art. no. 100334.
[116] K. Sun and Y. Kim. (Oct. 2020). *Considerations for ID/Location Separation Protocols in IPv6-Based Vehicular Networks*. Internet Engineering Task Force. [Online]. Available: https://datatracker.ietf.org/doc/draft-kjsun-ipwave-id-loc-separation/03/
[117] S. Chen, Q. Li, Y. Wang, H. Xu, and X. Jia, "C-V2X equipment identification management and authentication mechanism," *China Commun.*, vol. 18, no. 8, pp. 297–306, Aug. 2021.
[118] C. Li, "Automatic vehicle identification (AVI) system based on RFID," in *Proc. Int. Conf. Anti-Counterfeiting, Secur. Identificat.*, Jul. 2010, pp. 281–284.
[119] R. Zhang, X. Wang, P. Cheng, and J. Chen, "A novel pseudonym linking scheme for privacy inference in VANETs," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.
[120] A. Weimerskirch, "V2X security & privacy: The current state and its future," in *Proc. ITS World Congr.*, Orlando, FL, USA, 2011, p. 21.
[121] *Intelligent Transport Systems (ITS); Security; Pre-Standardization Study on Pseudonym Change Management*, Standard ETSI TR 103 415, 2018.
[122] S. Rüsch, K. Bleeke, I. Messadi, S. Schmidt, A. Krampf, K. Olze, S. Stahnke, R. Schmid, L. Pirl, R. Kittel, A. Polze, M. Franz, M. Müller, L. Jehl, and R. Kapitza, "ZugChain: Blockchain-based juridical data recording in railway systems," in *Proc. 52nd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2022, pp. 67–78.
[123] R. Kurachi, T. Katayama, T. Sasaki, M. Saito, and Y. Ajioka, "Evaluation of automotive event data recorder towards digital forensics," in *Proc. IEEE 95th Veh. Technol. Conf.*, Jun. 2022, pp. 1–7.
[124] K. F. Tasneem, G. Singh, P. Ahmed, S. Halder, S. Ganguly, S. P. Soni, and M. Rakhra, "Affordable black box: A smart accident detection system for cars," in *Proc. 9th Int. Conf. Rel., INFOCOM Technol. Optim.*, Sep. 2021, pp. 1–5.
[125] D. Bodson, "Black box—A new tool in fighting fraud," *IEEE Veh. Technol. Mag.*, vol. 4, no. 4, pp. 90–93, Dec. 2009.
[126] J. R. S. Scarpari, C. S. Deolindo, M. A. A. Aratanha, M. W. Ribeiro, A. de Souza, E. H. Kozasa, D. Hirata, J. E. Matieli, R. G. A. da Silva, and C. H. Forster, "Method for the synchronization of data recorders by coupling accelerometer data," in *Proc. IEEE Int. Symp. Inertial Sensors Syst.*, Mar. 2021, pp. 1–4.
[127] G. Falco, G. Falco, J. E. Siegel, and J. E. Siegel, "A distributed 'black box' audit trail design specification for connected and automated vehicle data and software assurance," *SAE Int. J. Transp. Cybersecur. Privacy*, vol. 3, no. 2, pp. 97–111, Oct. 2020.
[128] B. Shao, G. Bian, Y. Wang, S. Su, and C. Guo, "Dynamic data integrity auditing method supporting privacy protection in vehicular cloud environment," *IEEE Access*, vol. 6, pp. 43785–43797, 2018.
[129] M. Cui, D. Han, J. Wang, K.-C. Li, and C.-C. Chang, "ARFV: An efficient shared data auditing scheme supporting revocation for fog-assisted vehicular ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15815–15827, Dec. 2020.
[130] H. Yu, Z. Yang, S. Tu, M. Waqas, and H. Liu, "Blockchain-based offline auditing for the cloud in vehicular networks," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 3, pp. 2944–2956, Sep. 2022.
[131] F. Guo, Y. Qian, and W. Li, "Vehicle speed accident reconstruction based on event data recorder," in *Proc. 2nd World Conf. Mech. Eng. Intell. Manuf. (WCMEIM)*, Nov. 2019, pp. 722–727.
[132] C. A. Vinifred and A. S. A. Anand, "Event data recorder and transmitter for vehicular mishap analysis based on sensordrone," in *Proc. Int. Conf. Commun., Comput. Internet Things (IC3IoT)*, Mar. 2022, pp. 1–4.
[133] C. Sexton and J. Callenes, "Tiny black boxes: A nano-drone safety architecture," in *Proc. 52nd Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Workshops*, Jun. 2022, pp. 12–19.
[134] S. Escher, M. Sontowski, K. Berling, S. Köpsell, and T. Strufe, "How well can your car be tracked: Analysis of the European C-ITS pseudonym scheme," in *Proc. IEEE 93rd Veh. Technol. Conf.*, Apr. 2021, pp. 1–6.
[135] P. Kamat, A. Baliga, and W. Trappe, "Secure, pseudonymous, and auditable communication in vehicularad hocnetworks," *Secur. Commun. Netw.*, vol. 1, no. 3, pp. 233–244, May 2008.
[136] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proc. 1st ACM Int. Workshop Quality Service Secur. Wireless Mobile Netw.* New York, NY, USA: Assoc. Comput. Machinery, 2005, pp. 79–87, doi: 10.1145/1089761.1089775.
[137] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Netw.*, vol. 27, no. 5, pp. 48–55, Sep. 2013.
[138] N. Gruschka and M. Jensen, "Attack surfaces: A taxonomy for attacks on cloud services," in *Proc. IEEE 3rd Int. Conf. Cloud Comput.*, Jul. 2010, pp. 276–279.
[139] S. T. Alshammari, K. Alsubhi, H. M. A. Aljahdali, and A. M. Alghamdi, "Trust management systems in cloud services environment: Taxonomy of reputation attacks and defense mechanisms," *IEEE Access*, vol. 9, pp. 161488–161506, 2021.
[140] A. Guerna, S. Bitam, and C. T. Calafate, "Roadside unit deployment in Internet of Vehicles systems: A survey," *Sensors*, vol. 22, no. 9, p. 3190, Apr. 2022.
[141] P. B. Ulhe, A. Sinha, V. M. Dixit, V. V. Bhoyar, G. V. Gawali, and S. A. Nawkhare, "V2V communication: A study on autonomous driving using VANET and telematics," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Feb. 2020, pp. 806–809.
[142] R. Yee, E. Chan, B. Cheng, and G. Bansal, "Collaborative perception for automated vehicles leveraging vehicle-to-vehicle communications," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 1099–1106.
[143] *IPv6 Security, Cybersecurity, Blockchain*, Standard ETSI GR IP6 031, 2020.
[144] V. Mullet, P. Sondi, and E. Ramat, "A blockchain-based confidentiality-preserving approach to traceability in industry 4.0," *Int. J. Adv. Manuf. Technol.*, vol. 124, pp. 1297–1320, 2023.
[145] Y. Wang and A. Kogan, "Designing confidentiality-preserving blockchain-based transaction processing systems," *Int. J. Accounting Inf. Syst.*, vol. 30, pp. 1–18, Jan. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1467089518300794
[146] (2019). *Road Safety: Commission Welcomes Agreement on New EU Rules to Help Save Lives*. Accessed: Jul. 1. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1793
[147] *Threat, Vulnerability and Risk Analysis*, Standard ETSI TR 102 893, 2017.

CHAIMA ZIDI received the computer engineering and master's degrees from the National School of Computer Science (ENSI), Tunisia, in 2010 and 2011, respectively, and the Ph.D. degree in computer science and networks from Sorbonne Paris Cité University (Paris Descartes University), in 2018. Formerly as a Research Engineer with IMT Paris, she joined the University of Littoral as a Postdoctoral Researcher, in 2022. She is currently a Research Engineer with IMT Nord Europe. Her current research interests include the cybersecurity of vehicular communications, network performance assessment, and optimization.

PATRICK SONDI received the M.Sc. and the Ph.D. degrees in computer science from the University of Valenciennes, in 2007 and 2010, respectively, and the Habilitation ã Diriger des Recherches (H.D.R.) from the University of the Littoral Opal Coast, in 2020. He has been a Professor with IMT Nord Europe, since 2022. He joined the University of the Littoral Opal Coast as an Associate Professor, in 2013. His research interests include protocol engineering, the quality of service, safety, the security and event-based simulation of wired and wireless networks, especially in their application in industrial and transportation systems.

NATHALIE MITTON received the M.Sc. and Ph.D. degrees in computer science from INSA Lyon, in 2003 and 2006, respectively, and the Habilitation à Diriger des Recherches (H.D.R.) from Université Lille 1, in 2011. She has been an Inria Full Researcher, since 2006, and since 2012, she has been the Scientific Head of the Inria FUN Team, which designs protocols for wireless communications in constrained networks. Her research interests include self-organization from PHY to routing for wireless constrained dynamic and mobile networks. She has been nominated as one of the ten women stars in computer science, in 2020, by the IEEE Communication Society. She has published her research in more than 40 international revues and more than 120 international conferences. She coordinates the Horizon Europe SLICES-PP Project, participates in different Horizon Europe Projects (CyberSANE and NEPHELE), and in several program and organization committees, such as Infocom, since 2019, PerCom, since 2018, DCOSS, since 2018, Adhocnow, since 2015, ICC, since 2015, and Globecom, since 2017. She also supervises several Ph.D. students and engineers.

MARTINE WAHL received the Engineering degree in electronics from Polytech Paris-Sud, France, in 1991, and the Ph.D. degree from the Grenoble Institute of Technology, in 1997. She joined the Université Gustave Eiffel as a full-time Researcher in embedded communication, in 1998. Her research interests include communication protocols for wireless ad hoc systems and onboard communication systems in the context of vehicular distributed applications.

AHMED MEDDAHI received the master's degree from the University of Lille, France, the Ph.D. degree from the University of Evry-Paris Saclay, and the H.D.R. (accreditation to supervise research) from UPMC Paris 6 (Sorbonne University). He is currently a Professor with IMT Nord Europe. His research interests include the quality of service, context aware management, to network performance, and security. His current research interests include network security, resiliency, and performance in constrained and virtualized networks. He has published more than 35 research papers (international conferences, journals) two books. He is also involved in several international conferences committees and research projects (industrial and academics).