Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and Artificial Intelligence

Gueltoum Bendiab, Amina Hameurlaine, Georgios Germanos, Nicholas Kolokotronis & Stavros Shiaeles

Abstract
The arrival of autonomous vehicles (AVs) promises many great benefits, including increased safety and reduced energy consumption, pollution, and congestion. However, these engines have many security and privacy issues that could undermine the expected benefits if not addressed. AVs will provide new opportunities for hackers to carry out malicious attacks, posing a great threat to the future of mobility and data protection. The research trend in this field indicates that combining Blockchain and AI could bring strong protection for AVs against malicious attacks. Blockchain and AI have different working paradigms, but when merged, they can empower each other, and solve many security and privacy issues of AVs. AI can optimise the construction of the Blockchain to make it more efficient, secure and energy-saving, where Blockchain provides data immutability and trust mechanism for AI-based solutions and makes them more transparent, trustful, and explainable. Although some research is being conducted on this area, the topic of applying Blockchain and AI for securing AVs is not deeply investigated. In this paper, we explore the possible application of an amalgamation of Blockchain and AI solutions for securing AVs. We first introduce a classification of security and privacy threats that may arise from the application of AVs. Then, we provide an overview of recent literature regarding Blockchain and AI usage for securing AVs. Finally, we highlight limitations and challenges that may face the integration of Blockchain and AI with AVs based on our systemic review and suggest potential future directions for research in this field.

Index Terms
Autonomous vehicles, artificial intelligence, blockchain, privacy, cybersecurity, cyberattacks

Manuscript received 25 February 2022; revised 21 August 2022 and 10 November 2022; accepted 4 January 2023.

Acknowledgment
This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant 957406 and Grant 101021936. The work reflects the authors' view and the Agency is not responsible for any use that could be made from the information it contains. The Associate Editor for this article was H. H. Song. (Corresponding author: Gueltoum Bendiab.)

I. INTRODUCTION

Recently, Autonomous Vehicles (AVs) technology is attracting a lot of attention in both industry and academia, and has already been implemented by many automotive industries, such as Uber, Google, Apple, Aptiv, BMW, Tesla and Toshiba [1]. This technology enables driving automation systems to assist/replace human drivers in controlling the vehicle with butter driving skills, which greatly helps in reducing energy consumption, pollution, congestion and road accidents [2], knowing that around 94% of crashes are due to human error [3]. According to ABI Research [4], more than 30 million new AVs were sold in 2020, and by 2025, more than 115 million connected autonomous cars will be delivered by the global auto industry, nearly four times more than in 2020. Another recent study predicts that by 2030, one in 10 vehicles will be fully automated globally [5], but before integrating these engines into our transportation systems, there are several issues that need to be fully resolved. Of course, security and privacy are among the most important concerns of this new technology. In reality, AVs are vulnerable to various cyberattacks, which is a big challenge for the entire research community. A single compromised component can impact the hole in-vehicle network and lead to major safety losses that could potentially put human lives at stake [1]. For instance, malicious manipulation of Global Positioning System (GPS) data (e.g., GPS spoofing attacks) can affect the localisation of the AV and cause traffic accidents [2]. Moreover, hackers can prevent access to a fleet of connected AVs unless a ransom is paid, which could have a troubling effect on both automotive companies and customers using their vehicles [6].

In addition to security and safety concerns, AVs also have issues related to data privacy and protection. Hackers can have access to a huge amount of sensitive personal data that is collected and stored by the AV with relative ease. This may include information about location, biometric data and passwords for connected devices [7]. Industry players and security experts agree that cybersecurity and privacy challenges in the automotive industry are becoming increasingly important as AVs become a reality [1], [8]. For this reason, identifying attacks and defences against connected AVs has become one of the most active areas for researchers. In recent years, significant research efforts have been carried out to study vulnerabilities and major security attacks on connected AVs and available security countermeasures [1], [7], [8], [9], [10]. However, there is a lack of comprehensive reviews related to effective security and privacy countermeasures. In this context, many researchers in this field have argued that Artificial Intelligence (AI) and Blockchain (BC) can be used to effectively defend AVs attacks [2], [11], [12], [13]. BC has shown a notable ability to prevent cyberattacks completely without any failure in the past decade, while AI has proved to be more efficient and faster than traditional security approaches in detecting and dealing with cyber threats [2], [12]. However, the interrelationship between BC and AI is still a largely undiscovered area, and there is a lack of comprehensive surveys on efforts made in recent years addressing AVs security and privacy issues using BC and AI techniques. Thus, the motivation behind this paper is to explore the possible application of an amalgamation of BC and AI solutions for securing intelligent AVs, through an extensive overview of existing and new applicable solutions. The key contributions of this paper go beyond existing studies in terms of the following aspects:

• Comprehensive analysis of the major vulnerabilities and issues related to AV security and privacy based on current literature in this field. Since detailed studies that focus on security and privacy issues related to AVs are fairly new, we propose a classification of the most critical cyberattacks on both AV components and communication channels based on current literature and recently reported attacks to help researchers improve AVs security and make them more resistant to cyberattacks.
• Critical review of the recent solutions employed to protect AVs against cyberattacks based on BC, AI, or an integration of both techniques. This will help researchers to understand how BC and AI can offer solutions for protecting and securing AVs. To our best knowledge, this work is the first that proposes a detailed review of these studies and explores the benefits and challenges of combining BC and AI for securing AVs.
• Discussion of open issues and challenges related to combining BC and AI with AVs and highlights future research directions that can help researchers in this field to explore and tackle the pressing challenges for making AVs more safe, secure, and privacy-preserving.

Overall, this paper represents an effort of understanding how BC and AI can make AVs more safe, secure and privacypreserving. The remainder of this paper is structured as follows: Section II presents the key components of AVs and their communication networks, while Section III presents a classification of security threats based on recent literature in this field. Section IV presents a critical review of AVs security and privacy solutions using AI and BC and analyses the feasibility of the combination of BC and AI. Section V discusses the open issues and challenges related to combining BC and AI with AVs and finally, Section VI concludes the paper and outlines directions for future research.

II. AUTONOMOUS VEHICLES BACKGROUND

The arrival of new technologies and more optimized communication systems has led to the creation of autonomous or self-driving vehicles, with greater functionality and better levels of autonomy. These vehicles use information gathered from internal systems and the external environment, Machine Learning (ML) systems and powerful processors to provide useful

Insert Fig. 1 here

driving assistance and improve convenience and safety [14]. The term autonomous is usually used interchangeably with self-driving. However, there is a slight difference between the two terms. Based on the Society of Automotive Engineers (SAE) definitions for the levels of automation for vehicles [15], which have been adopted by the U.S. Department of Transportation, there are 6 levels of automation ranging from level 0 (no automation) to level 5 (full automation), each level with an increasing amount of automation and a decreasing amount of driver involvement (see Fig. 1). From levels 0 to 2, a human driver monitors the driving environment, whereas from Levels 3 to 5, an Automated Driving System (ADS) monitors the driving environment and the human is not fully involved (such as being hands-off). Thus, based on SAE definitions [15], an autonomous vehicle at levels 4 and 5 is self-driving, but a self-driving vehicle at level 3 is not autonomous as it is limited in the operating environment and requires

the involvement of a human driver that can take control when needed. From level 3 onwards, the vehicle must be equipped with an increased number of sensing and communicating devices in order to be “self-aware” [8]. Actually, fully autonomous vehicles are still unavailable for the general public except at special trial programs (e.g., Google and Tesla self-driving cars), however, analysts predict that by 2030 these vehicles will be in use in cities and urban areas [5].

In general, an AV could be defined as a specific type of Internet of Things (IoT) system and also a kind of Cyber-Physical System (CPS) that is composed of a collection of complex interconnected embedded system components [16], [17]. It differs from conventional vehicles by using various automotive sensors (e.g., radar, camera, and LiDAR (Light Detection and Ranging)), actuators, and Electronic Control Units (ECUs) connected to an onboard computer that accomplishes the role of the human driver in navigating the vehicle [1], [18]. The AV’s sensors are responsible for sensing the vehicle’s dynamics (e.g., the vehicle location) and its surrounding environment (e.g., road traffic status, etc.) [18]. The computer processes the sensors data and commands the ECUs, which control their corresponding actuators accordingly to achieve a specific function [18]. The connections between the onboard computer, external sensors, ECUs, and actuators form an in-vehicle network [16]. AVs are also able to transmit and receive data from other vehicles, road infrastructure, Internet

Insert Fig. 2 here

and also pedestrians by using the Vehicle-to-Everything (V2X) communication technology [16], [18]. All these components represent attack surfaces that malicious actors can exploit in order to get unauthorized access to the AV [8], [18]. In this paper, we have identified four key components in order to explore the security and privacy aspects of AVs. These components are; (a) sensing components, (b) ECUs, (c) in-vehicle network and (d) V2X network.

A. Sensing Components

Sensors are key components for autonomous driving: they allow the vehicle to monitor its surrounding environment, as well as collect the data needed in order to drive safely [17]. In this context, analytics predict that connected AVs can generate up to 25 GB of data per hour, but in the future, especially with increasing levels of automation, they will likely generate over 300 TB of data per year [19]. Generated data is processed and analysed by an onboard computer in order to build a path from one point to another and to send the appropriate instructions to the controls of the AV, such as steering, change speed, and braking [8], [18]. As illustrated in Fig. 2, the three primary AV sensors are cameras (mono and stereo cameras), LiDAR and RADAR (Radio Detection and Ranging technology) [16]. These three sensors together provide the vehicle visual of its surrounding environment and help it detect the speed and distance of nearby objects [8], [17].

The RADAR sensor uses radio waves for object detection within a certain range. It is used in AV to recognize the environment of a vehicle in real-time [18]. LiDAR uses a shorter wavelength laser to achieve higher measurement accuracy and better spatial resolution than RADAR. Video cameras read traffic lights and road signs and monitor pedestrians and obstacles. The global

navigation satellite system (GNSS) is the most widely used technology for providing accurate position information on the surface of the earth. The best-known GNSS system is the Global Positioning System (GPS), which provides Positioning, Navigation, and Timing (PNT) services to the users. The operating principle of the GNSS is based on the ability of the receiver to locate at least four satellites, to calculate the distance to every single one of them, and then use this information to identify its own location by using a process called trilateration. Ultrasonic sensors are used to measure distances between the sensor and an object using high-frequency sound waves. These sensors have the capability to detect objects that are solid, liquid, granular, or in powder form. Ultrasonic sensors are typically used in shortdistance applications, such as a parking assistance system in a vehicle [21]. Additionally, other sensors, including odometry and Inertial Measurement Unit (IMU) sensors, are used to determine the relative and absolute positions of the vehicle.

B. Electronic Control Units

The Electronic Control Unit (ECU) is an embedded system that controls the state of the automatic transmission of the vehicle engine and manages the sensors inside the vehicle. Typically, small and medium-sized vehicles include approximately 50 ECUs [21], while modern luxury vehicles can integrate as many as 150 ECUs [22]. Every ECU in the vehicle is responsible for controlling a specific function, such as body control, brakes control, seat control, and door/window control, among others. ECUs contain several modules, including the general electronic module (GEM), central control module (CCM), engine control module (ECM), brake control module (BCM), transmission control module (TCM), powertrain control module (PCM), body control modules (BCM), and others [23]. An ECU collects information from one or more vehicle sensors and uses it to take action if necessary. An airbag ECU, for example, collects data from crash sensors and seat sensors. When a collision occurs, the ECU determines which airbags to deploy based on where the passengers are seated, and directs the actuators to deploy them [1].

The body control module mainly takes care of the comfort and security features of the car. It includes modules for the door, seat, power lock, airbag, air condition system, and light control [21]. TCM is mainly responsible for automatic transmissions of data from sensors and the engine control unit. Whereas, the powertrain control module combines the functions of the engine control unit and transmission control unit [1], [21]. All ECUs are connected as nodes through a physically conventional two-wire bus, which transmits differential wired-AND signals. The On-Board Diagnostic (OBD) connection port (standards OBD-I and OBD-II) is mainly used in Controller Area Network (CAN) to retrieve diagnostic data such as voltage, fuel level, and speed from the AV components and its ECUs. It is also used by many manufacturers to update or modify the software (or firmware) embedded in the ECUs [9], [21]. Currently, the OBD-II port is adopted by all automotive manufacturers and a large number of wireless OBD-II dongles are developed, enabling vehicle owners to perform remote vehicle functions from mobile apps [24].

C. In-Vehicle Network

An in-vehicle network realizes the transmission of status information and control signals among sensors, actuators and electronic units (ECUs) in the AV. In [25], a survey on networking and

communication technologies in autonomous driving is provided. Authors divide the in-vehicle network into wired and wireless technologies. Wired technology includes the controller area network (CAN), local interconnect network

Insert Fig. 3 here

(LIN), FlexRay, Ethernet, Media-Oriented Systems Transport (MOST), Intelligent transport system Data Bus (IDB-1394), Digital Data Bus (D2B), Low Voltage Differential Signaling (LVDS), and PowerLine Communication (PLC). According to the authors, the use of wired technology has many limitations; especially with the increasing complexity of the AV design: (i) the internal wiring harness becomes highly complex; (ii) wire materials and wiring layout design turn more costly; (iii) the deployment of wires becomes limited, for example, it is not appropriate to use the wired structure on steering wheel and tire parts; and (iv) the intra-vehicle space will become more congested. Traditional wireless technologies are used to establish wireless connections between personal electronic products and the infotainment systems on-board. Using wireless interconnection to transmit data generated by a variety of sensors, actuators or ECUs, can greatly reduce the need for wires and the weight of the AV's bodywork, save energy, and the sensors can be integrated into various parts of the vehicle that cannot be wired. Wireless technologies that have been used or maybe widely deployed in AVs in the future can include Bluetooth 5.0, ZigBee, Ultra WideBand (UWB), and Wireless Fidelity (WiFi). It is unclear whether they are less expensive than wired communication systems. Moreover, the performance of wireless communications may be affected by the complex electromagnetic environment. Therefore, additional study into the wireless interconnection scheme in autonomous driving is required [25].

D. Vehicle-to-X Communication Technology

Vehicle-to-everything or Vehicle-to-X (V2X) technology enables AVs to communicate with their surroundings and makes driving safer and more efficient for everyone. As shown in Fig. 3, V2X technology consists of V2V (vehicleto-vehicle), V2I (vehicle-to-infrastructure), V2P (vehicle-topedestrian) and V2N (vehicle-to-network). V2V refers to the direct communication between vehicles, V2I is the connection between vehicles and infrastructures, V2P is the mutual communication between vehicles and pedestrians or other vulnerable road users like cyclists, and V2N connects vehicles to the Internet [25]. Vehicle ad-hoc networks (VANETs), which are special class of Mobile Ad Hoc Networks (MANETs), are an area of significant interest for researchers of V2X communications. VANET is a combination of wireless ad-hoc network and cellular technology which yields an Intelligent Transport System (ITS) between vehicle to vehicle and vehicle to Road-side units (RSUs) [26]. It uses dedicated short-range communications (DSRC) which are based on the IEEE 802.11p standard for wireless access in vehicular environments [21], [27]. DSRC technology supports a short exchange of information among DSRC devices such as On-Board Units (OBUs) equipped inside the vehicle, RSUs and mobile devices carried by pedestrians [28]. The RSU communicates with location servers through a wired/wireless network for tracking information on all vehicles. The service infrastructure of an RSU includes the traffic-management system, public-key infrastructure, and RSU management centre [21].

The mobile cellular network is another communication structure required for V2X. In June 2017, the mobile industry body 3GPP [29] standardised a set of technologies, known as Cellular Vehicle-to-Everything (C-V2X), specifically designed to enable communications between AVs and roadside infrastructure. Based on LTE networks, C-V2X provides one solution for integrated direct communication (V2V, V2I and V2P) with network communication (V2N) by leveraging existing cellular network infrastructure. C-V2X can support a wider range of capabilities than earlier dedicated vehicle connectivity solutions that are based on 802.11p. It supports both short-range and long-range transmissions, and enables highly reliable, real-time communication at high speeds and in high-density traffic [30]. In the V2V, V2I and V2P communications mode, C-V2X operates in the 5.9 GHz frequency band and works independently of the cellular networks. It uses GNSS as its primary source of time synchronisation in out of coverage scenarios. In the network communications mode, C-V2X employs the conventional mobile network to enable the vehicle to receive information about road conditions and traffic in the area [31]. Recently, 3GPP started to enhance C-V2X in several ways towards the 5G New Radio (NR) V2X specifications in Release 16 [32] and beyond.

V2X communication technologies can also be used to establish communication between AVs and Unmanned Aerial vehicles (UAVs) which can provide many services to ground AVs. Currently, UAVs are envisioned as an essential ingredient in realizing the next generation of intelligent transportation systems for connected AVs. Some of the critical applications that UAVs can provide to ground AVs include traffic monitoring by using UAV and edge computing devices, edge/fog computing services, incident or accident reporters and dynamic roadside units (RSUs) [33]. For instance, UAVs can act as mobile aerial base stations to assist AVs, resulting in an interconnected heterogeneous automated system. Further, because of their high mobility, UAVs can enhance the AVs' perspective and the visibility of their surrounding areas [33], [34].

III. MAJOR SECURITY AND PRIVACY THREATS FOR AUTONOMOUS VEHICLES

Autonomous Vehicles provide new opportunities for hackers and malicious actors to implement different successful cyberattacks that could lead to catastrophic incidents and cause major safety losses [1], [7], [9], [35]. Extensive research efforts have been made by the research community to identify vulnerabilities in these engines [1], [8], [21], [35], [36], [37], [38], and many studies have demonstrated successful scenarios of attacks on AVs and their components including sensing components, ECUs and communication channels [2], [39], [40], [41]. According to [9], the main common motivations of these attacks are to gain remote control over AVs, to steal important and confidential information that can be used for launching further attacks on AVs, or to interrupt the AVs operations by corrupting important components (e.g., Radar, LiDAR, ECUs, CAN bus, etc.) and making the autonomous driving mode unavailable [21], [35], [37], [38], [40]. Fig. 4 shows the most hackable points of AV and AV communication networks by which the attacks could land on the AV.

In this section, we present the most critical cyberattacks on both AV components and communication channels based on the current literature and recently reported attacks. As

illustrated in Fig. 5, we classify the major cybersecurity and privacy threats into the following main categories: manipulation-based attacks, identity-based attacks, servicebased attacks, software-based attacks, attacks targeting data and attacks through physical access to the AV system.

A. Manipulation-Based Attacks

The aim of this category of attacks is to gain unauthorized access to the AV in order to compromise the data integrity and violate the privacy of users. The following attacks are reported: Man-in-the-middle attacks, injection attacks, tampering attacks, overlay attacks and modification attacks.

1) Man-in-the-Middle Attacks: In this attack, malicious actors can intercept and manipulate the communications between AVs and external devices, which are usually established through WiFi, Bluetooth, ZigBee and mobile communication protocols [38]. For instance, attackers can take control of an AV, OBU or RSU and actively intercept, replay, and manipulate the messages transmitted between two entities (e.g., two AVs in V2V network, or RSU in V2I network), while both entities believe that they are in direct communications with each other [35], [36]. Authors in [42] successfully implemented a man-in-the-middle attack on a connected AV. After gaining access to the OBD port, the attackers were able to intercept data to and from the AutoPi Cloud interface and interrogate information about the AV and control key components such as the airbag control system.

2) Injection Attacks: This category refers to a broad class of attack vectors in which attackers try to supply untrusted and malicious input to the AV components, especially the control units (ECUs) that control the major components in the AV [9]. For instance, firmware in ECUs that is programmed based on modern operating systems, such as Linux and Android, is vulnerable to code injection attacks [9], [36], [38]. By injecting malicious code, these ECUs can behave normally while sending sensitive information from the AV to third malicious parties at the same time [9], [38]. The CAN bus, which does not have enough security features [9], [35], is also vulnerable to two forms of injection attacks. The one is injecting CAN diagnostic messages, and another one is injecting standard messages to intimate the messages from control units [9], [35].

3) Tampering Attacks: The aim of this attack is to deliberately modify (destroy, manipulate, or edit) data through unauthorized channels [43], [44]. Many studies have proven that AV sensing components are vulnerable to physical chip-tampering and data tampering attacks [9], [21], where attackers can easily

Insert Fig. 4 here

Insert Fig. 5 here

tamper with sensor readings to disrupt the normal operation of the AV. ECUs are also vulnerable to ECUs code tampering attacks (ECU firmware code tampering) [43], and ECUs reprogramming/flashing attacks, since the in-vehicular network give easy and non-secure

access to ECUs. Meanwhile, the issue of messages tampering has been noticed from the early days of V2V and V2X communications, where many successful message tampering attacks have been reported on VANET comprising of vehicles with autonomous Levels 1 to 4 [1], [35], [36], especially those related to traffic safety.

4) Modification Attacks: Such attacks are primarily considered as integrity attacks because they involve modification of data in real-time, but they could also represent availability attacks because they can affect the AV behaviour. For instance, authors in [45], exploited the invisible infrared lights (IR light) to implement a new security threat to the AV camera, called "I-Can-See-the Light" attack (ICSL Attack). By leveraging the IR light features, authors have successfully modified the environment perception results by generating invisible traffic lights, creating fake invisible objects and introducing SLAM (Environment Perception and Simultaneous Localization and Mapping) errors to the connected AV.

B. Identity-Based Attacks

Every AV is identified with a unique identifier that can help to recognise the AV and the exchanged messages [9]. Identitybased attacks are one of the most serious threats to connected AVs as they forge identities to masquerade as authorized entities, in order to get access to the AV components and manipulate them [9], [37], [40], [46], or to send falsified information through the V2V and V2I communication channels to disrupt AVs' operation and traffic flow [9], [35]. These attacks mainly target components that lack strong authentication methods, such as CANs and signals for sensors [9], [47]. The most critical cyberattacks in this category are; spoofing attacks, impersonation attacks, Sybil attacks, replay attacks, and passcode and Key attacks.

1) Spoofing (or masquerading) Attacks: The aim of this attack is to gain control over AVs by using false identities or sending false data [40], [48]. Examples of spoofing attacks are GPS spoofing, LiDAR spoofing, radar spoofing, GNSS spoofing and camera spoofing [37], [38]. In the case of GPS spoofing, attackers attempt to trick a GPS receiver by broadcasting false, but realistic GPS signals (e.g., fake time or location) [9], [11]. Similarly, a LiDAR Spoofing attack creates fake signals that represent an object and injects them into a LiDAR sensor. Researchers in [49] demonstrated that it is possible to deceive a moving AV and perform LiDAR point spoofing with alarming consequences. Radar spoofing attacks try to replicate and rebroadcast fake radar signals to inject distorted data into the sensor [9]. Authors in [48] have demonstrated two successful real-world scenarios of radar spoofing, in which the victim radar is spoofed to detect either a phantom emergency stop or a phantom acceleration.

2) Impersonation Attacks: In this kind of attack, an adversary tries to masquerade as a legitimate entity (e.g., by stealing the identity of a legitimate AV or using a fake identity) to perform unauthorized operations [9], broadcast falsified information, drop critical messages or inject malware [35]. Especially, in V2V networks, where neighbouring AVs periodically exchange Basis Safety Messages (BSMs) [40]. Thus, a malicious AV that connects with a spoofed identity can establish communications with the neighbouring AVs by sending fake messages and receiving sensitive data. For instance, an AV can claim several locations concurrently, which can

lead to traffic congestion. In this mode of attacks, a single identity is spoofed or created at a time [35].

3) Sybil Attacks: In Sybil attacks, a large number of identities are spoofed, or created, simultaneously in order to carry out several malicious operations [9], [21], such as spreading falsified information through the V2V and V2I communications to disrupt AVs' operation and traffic flow [35]. In 2018, a successful Sybil attack on Google's autonomous car led the car to show an incorrect GPS location and caused the vehicle to stop in the middle of the road [41]. In this scenario of attack, several fake nodes were successfully added to the network and sent misleading location and traffic condition information to the Google car by exploiting the routing table's flaws and non-encrypted messages of Google cars.

4) Replay Attack: The aim of this attack is to spoof the identities of two parties, intercept the exchanged messages, and relay them to their destinations without modification [46]. Several studies on the in-vehicle network have demonstrated that sensors channels and control systems in AVs are not resilient to replay attacks [35], [47], especially CAN protocols that do not support encrypting messages for authentication and confidentiality [9]. Therefore, attackers can gain access to the AV and observe all messages transmitted on the CAN bus, and therefore easily impersonate a control unit (ECU) and transmit fake messages through the OBD connection ports [9]. Replay attacks can also target communication channels between the vehicle and the RSUs or other neighbouring AVs in order to steal secret encryption keys or passwords and use them to authenticate themselves later [9], [35], [38], [46].

5) Passcode and Key Attacks: Passcode and keys are one of the safety features of connected AVs [9], [38]. Many studies have demonstrated that attackers can easily recover secret keys and passwords from connected AVs, RSUs or OBD by performing attacks such as brute force, dictionary, rainbow table, password theft and social engineering [9], [35], [36], [38], [46]. For instance, a brute force attack can crack the Bluetooth connectivity of a connected AV in a few seconds since the AV's Bluetooth pin has only four digits [35], [36]. Another form of attack, which has been observed, and can take place against any type of vehicle (not only connected AVs) using remote central locking, is replay attack of key signal. By re-using a stolen key signal wirelessly, an attacker could unlock the vehicle without having the original key–device in his possession [50].

C. Service-Based Attacks

The primary goal of service-based attacks is to interrupt the AV operations, or to disrupt the traffic flow in a large area. This category includes the following attacks.

1) Denial of Service Attack (DoS) and Distributed DoS: DoS/DDoS attacks are of the most dangerous threats that AVs may experience. In fact, several studies proved that DoS/DDoS attacks can be used to stop the in-vehicle key components, such as camera, LiDAR, Radar, CAN bus and ECUs, by an overload of processes [9], [11]. For instance, studies [51], [52] illustrated by experiments that the CAN protocol does not have any security measures against DoS attacks and showed how easy such an attack is. The experiments were performed with

cars that are currently in use. Authors in [52] confirmed that a DoS attack can overload the CAN network with irrelevant messages that may alter the AV behaviour, disrupt the vehicle control system, and even cause physical harm to drivers and passengers [38]. V2V networks are also vulnerable to DoS and DDoS attacks because they have limited connection bandwidth [9]. In this context, researchers in [53] demonstrated a successful botnet-based DDoS attack by exploiting BSM messages exchanged between AVs in V2V networks. The attack caused heavy congestion on a previously targeted road. DoS and DDoS attacks on V2I networks could be much more destructive and cause traffic flows disruptions in a large region [9], [11], [36], [40].

2) Jamming Attacks: This type of attack aims to prevent the AV from using V2V and V2I channels to communicate with other AVs as well as RSU stations, by causing intentional interference with noisy signals or messages [9], [36]. It can also target the AV sensors (GPS jamming [38], LiDAR jamming [9], radar jamming [9] and camera frequency jamming [36]) by injecting noise and crafted signals, which could cause blindness and AV malfunction [9], [36]. Authors in [54] validated by experiments several successful jamming and spoofing attacks on many ultrasonic sensors of several real car models with driver assistance system, including a Tesla Model S. The attacks were performed by using a DIY ultrasonic jammer with a low-cost Arduino in order to generate ultrasonic noises and cause continuing vibration of the membrane on the sensor, which makes the measurements impossible. Authors confirmed that when jamming attacks are launched, the obstacle can no longer be detected by all the tested vehicles, therefore no alarm is given to the driver.

3) Routing Attacks: The main features of the AV external networks (V2V and V2I) include high mobility, fastchanging network topology, absence of fixed security systems, open wireless communication medium and in some cases, a large number of vehicles on roads [25], [26]. These features make them vulnerable to routing attacks including black hole attacks [55], grey hole attacks, wormhole attacks [35], sinkhole attacks and rushing attacks [56]. The misbehaviour routing problem has been extensively discussed and investigated in the wired and wireless networks, but the security problem cannot be prevented completely [56], especially in the vehicular networks composed of vehicle nodes, which behave quite differently from other wireless nodes [35], [55], [57].

4) Sensor Blinding Attacks: This kind of attack targets the three primary AV sensors (camera, radar and LiDAR), which work together to provide the vehicle visuals of its surroundings. Each of these three sensors can be blinded, thereby hindering the AV's ability to retain full awareness of environmental conditions or potential obstructions [9], [58]. For instance, cameras may be blinded by a quick burst of extra light [21]. In [58], authors implemented a successful blinding attack on a MobilEye C2-270 camera installed on a non-automated car's windshield. In this scenario of attack, the authors used a quick burst of 650 nm laser to fully blind the camera and the camera never recovered from the blindness.

5) Spamming Attacks: The aim of this attack is to send a massive amount of unsolicited and SPAM messages through the network, thereby increasing the transmission latency and causing a severe delay in V2V and V2X communications [1], [38], [53], [59]. Security professionals warn

that spamming attacks could be a serious threat to the AV ecosystem due to the use of botnets (Spamming botnets), where numerous compromised nodes (e.g. AVs, RSUs, AV sensors, etc.) can be used to send large numbers of spam messages across the AV networks (e.g., VANETs) [1], [9], [53].

D. Software-Based Attacks

In addition to all the attacks mentioned above, there are many software-based attack vectors that pose undeniable security and privacy risks that must be addressed. This includes malware, ransomware attacks, mobile apps attacks [21] and attacks against the machine learning system [35].

1) Malware Attacks: One of the severe threats of the extensive introduction of automation in vehicles is vehicle hacking by using different forms of malware including viruses, worms, trojans, rootkits, backdoors, etc. [36], [52], [60], [61]. Malware can infect AVs through a variety of vulnerabilities, including wireless communication (Bluetooth, WiFi, Cellular and 5G), vehicle-based WiFi hotspots, internet connectivity and malware-infected devices [60], [61], [62]. In recent years, numerous research studies have demonstrated different methods by which malware can infect the AV systems [61], [63]. For example, in 2019, a group of white hats proved the ability to hack a Tesla Model 3 vehicle in few seconds by exploiting a weakness in the browser of the “infotainment” system to get inside the vehicle’s computers and run their own source code [64]. Another research group at Leuven in Belgium were able to steal a Tesla Model X vehicle by injecting malware through the firmware update into the key fob via Bluetooth connection [65]. In [63], authors demonstrated the first remote car-hacking against a Chevy Malibu vehicle by exploiting a weakness of the Bluetooth stack. The malware is injected into the vehicle by synchronising their mobile phones with the radio of the vehicle. Then, the inserted malicious code was able to send messages to the ECU of the vehicle that could lock the brakes. Simulation studies in [52], [66], [67], and [53] showed that malware can spread to many AVs through V2V and V2X communication channels and turn these AVs into malicious bots, thereby creating a botnet network.

2) Ransomware Attacks: The term ransomware, which is a mash-up of the words malware and ransom, covers all cyberattacks that use computer malware (e.g., virus, trojan horse, worm, rootkit, etc.) to infect a computer system so that the attacker can then try to extort something from the victim such as paying a ransom [68]. Security professionals expect that ransomware attacks will be a major security threat for AI-based self-driving vehicles, mainly for commercial vehicles [36], [60], [69]. In 2017, Honda Motor Company, one of the largest automobile manufacturers in the world, was subject to a major WannaCry ransomware attack, in which lots of Honda self-driving cars have been hindered to get software updates during the ransomware attack [70]. In [69], authors demonstrated by experiments potential hybrid crypto-ransomware attacks on the in-vehicle infotainment systems. In these experiments, authors showed how AV ransomware will differ from traditional ransomware and identified a set of constraints on vehicular ransomware.

3) Attacks on Machine Learning: Machine Learning (ML) and Deep Neural Networks (DNNs) are essential in AVs for processing sensory data and making informed decisions at different levels [9], [36], [71]. However, these techniques have been recently found vulnerable to several attacks that attempt to manipulate the learning system and lead it to produce an incorrect result [44]. The most well-known attacks are evasion, poisoning and inference [44], [63], while there are also trojaning, backdooring and reprogramming attacks [9], [71]. Adversarial poisoning attacks target the data used to train the learning system by introducing poisoned data into the training dataset [44]. However, adversarial evasion attacks attempt to trick the learning system at the testing stage by providing deceptive real-time input [71]. Adversarial Attacks can only add new data to the existing dataset or modify it, but they do not have access to the model and initial dataset [44], [71]. Regarding trojaning, attackers still do not have access to the initial dataset, nevertheless, they have access to the predictive model and its parameters and can for example retrain this model. As for inference, attackers intend to explore the learning system, such as model, or dataset that can further come in handy. Backdooring is a new class of attacks on DNNs that combine poisoning and trojaning [72]. However, attackers not only inject additional behaviour, but they do so in such a way that the backdoor operates after retraining the system [44], [72]. Adversarial reprogramming attacks are based on remote reprogramming of the neural network algorithms with the use of well-crafted perturbations on the input data [73].

Recently, several real-world scenarios of attacks have been successfully performed on the vision system of AVs, which has led the learning system to make mistakes [25], [44], [74], such as misclassification of traffic signs [75]. This has raised many privacy and security concerns about the use of such methods in AVs, especially in fully automated vehicles [36], [40], [44]. 4) Mobile Apps Attacks: Autonomous vehicles and their ecosystems are connected to mobile applications, through which their owners have the ability to remotely control fundamental operations of the vehicle [9], [21], [61]. These applications, which are normally installed on mobile phones, iPads or tablets, are prone to various cyberattacks. Using these mobile applications, attackers may gain unauthorized access to the vehicles, their ecosystems and the data processed in them, practically being able to perform any kind of malicious activity [21], [24], [61]. Security experts from Kaspersky found that mobile apps from car manufacturers available from app stores lack sufficient security and can be used by hackers to get the GPS coordinates of a connected AV, trace its route, open its doors, steal the vehicle or even disable it [76].

E. Data Privacy

Autonomous vehicles by their very nature would generate, collect, process and store a massive amount of data that can identify, with a high degree of certainty, the owner or passenger of the vehicle, their activities, location, direction of travel and journey history [77]. This data will have great value to hackers, advertisers, insurance companies and many other service or product providers [77], a situation that creates various security and privacy fears, not only because of the huge amount of data collected, and stored, either in the vehicle itself or sent to the cloud, but also because it remains unclear who owns the generated data and if further transmissions take place [78]. Specific threats, which have an effect on privacy aspects of AVs have been deeply investigated in [78], [79], [80], and [77].

1) Location Trailing Attacks: This passive attack constitutes a critical threat to the privacy of users as well as con?dentiality of transmitted messages, since attackers can obtain private and sensitive data of the owner and passengers through location and tracking of the AV activities as well as the driving record [9], [35]. For example, determining that the user visited an ATM and/or shopped at an expensive store provides the possibility of targeted theft [8]. In addition, with the help of location information, attackers can profile, predict, and possibly manipulate the behaviour of AV users [35]. In fact, many studies demonstrated that attackers can track any AV of interest and violate privacy of the drivers and passengers [1], [8], [35], [67], [81]. In [67], authors demonstrated a global-scale location trailing attack that is performed by AVs themselves. For that, authors have created a vehicular botnet by compromising multiple vehicles and organizing them into a botnet. The vehicular botnet communication is concealed inside BSM broadcasts. Authors proved that the vehicular botnet is effective even against the best existing pseudonym changing scheme used by AVs, where the attack can keep a vehicle under surveillance up to 85% of its route, and identify its destination address 90% of the time.

2) Eavesdropping Attacks: This type of attack, also known as sniffing or snooping attack, involves the interception and/or theft of sensitive information transmitted over a communication channel (e.g., AV identity, current AV position, speed, acceleration, and CAN messages) [8], [36], by taking advantage of the insecure communications and unencrypted protocols in the AV networks (in-vehicle networks and external networks (V2V and V2X)) [8], [82]. Stolen information can help to access other information on the network and to launch further attacks such as identity-based attacks. Eavesdropping is also a passive attack, and hence is difficult to detect, especially in broadcast wireless communication [1], [35], [83].

3) Traffic Analysis Attacks: Similar to eavesdropping attacks, the purpose of traffic analysis attacks is to passively collect valuable data about the target victim (e.g., AV ID, AV location, route travelled, etc.), but without compromising the actual data [9], [84]. This data can be further analyzed to perform further attacks against the target victim, such as jamming, eavesdropping, location trailing and Sybil attacks [1], [84]. This attack presents a high-level threat to user privacy and to data confidentiality in vehicular communication as it aims to break the anonymity of the communications between vehicles (V2V) and with the RSUs (V2I) [1], [46].

4) Home Attacks: This is a new class of attacks against privacy and data confidentiality, where attackers hijack control of the vehicle from another user on the network, through the Internet connection [85] and gain unauthorized access to important information about the vehicle (e.g., its location, owner's identity, etc.). In the worst-case scenario, attackers can gain full control over the vehicle and use it to perform their malicious operations such as broadcasting wrong messages, stealing valuable and sensitive data, changing sensors' behaviour, or launching further attacks that can affect the whole network [1], [81], [84].

F. Physical-Access Attacks

AV has many direct and indirect physical interfaces that can become potential surfaces of attacks because they give the attackers direct access to the in-vehicle network, especially the CAN bus and subsequently access to the control units (ECUs) [51], [61]. These interfaces are

vulnerable to attack due to their lack of security features, such as authentication scheme, access control and verification process [9], [35], [61].

1) Direct Access Attacks: Certain attacks could be performed by those with direct physical access to the vehicle. For instance, vehicular systems that are exposed to passengers, such as USB ports or OBD-II ports, might provide mechanisms to allow for malicious use or exploitation [9], [51], [58], [60], [62]. The OBD system is the primary attack surface because it can provide direct access to the vehicle's control units (ECUs) and its internal network busses through the OBD-II port and the OBD dongles [24], [61]. In [24], authors identified five different types of vulnerabilities in wireless OBD-II dongles, which are used to perform remote functions on vehicles through mobile apps, with 4 being newly discovered.

2) Indirect Access Attacks: The in-vehicle network can also be accessed through indirect interfaces without the presence of the attacker [61]. In fact, most connected vehicles nowadays offer indirect physical access through electronic devices such as multimedia devices (CD, USB driver, or MP3 player), cell phones, iPads, and laptops [1], [41], [62]. For instance, these devices can be abused by malware to infect an AV with the possibility of extending such attacks to multiple vehicles [9], [21], [40], [60]. Bluetooth, Remote Keyless Entry and Tire pressure also provide indirect physical access to the AV network that could be exploited by hackers and malicious actors [62]. In [86], authors successfully implemented four indirect access scenarios of attack to the CAN network through a multimedia disc. In another similar study [63], authors demonstrated several indirect access attacks to the CAN bus of the vehicle via different multimedia devices, including computer, CD, USB driver and MP3 player.

Throughout this section, we presented an extensive list of potential threats related to the security and privacy of autonomous vehicles. As AVs are experimental at this time, there is little empirical evidence of real cyberattacks against these connected engines. However, all the attacks mentioned above lead to the conclusion that securing these vehicles and business models is of great importance. Solutions to these issues may be provided through the application of AI and BC, which are the topics discussed in the next section.

IV. INTEGRATION OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE WITH AUTONOMOUS VEHICLES

With the proliferation of cyberattacks against autonomous vehicles, several defensive techniques are being explored [2]. Blockchain (BC) and Artificial Intelligence (AI) are certainly the two cutting-edge technologies which, when merged, might bring strong security protection for connected vehicles against malicious cyberattacks [1]. In this section, we review recent literature proposing security and privacy-preserving solutions for connected AVs. First, we discuss the solutions offered by utilising BC techniques, then by AI models, and finally by combining both technologies.

A. Literature Review on Blockchain Techniques

Blockchain is a kind of distributed, immutable ledger of transactions that is duplicated and distributed across the entire network of participating nodes [13], [87]. Each block in the chain is composed of a cryptographic hash of the previous block, a timestamp and a number of transactions that are generally represented as a Merkle tree [88]. Multiple parties, usually called miners, can jointly maintain the ledger through a specific consensus algorithm so that, the stored data on the chain has the features of decentralised and powerful consistency [88]. The consensus algorithm is the key procedure through which all the participating nodes in the network can reach a common agreement upon the total order of the transactions [87]. Moreover, a BC network could be public, private or consortium [13], [88]. In a public BC, such as Ethereum [89], Litecoin [90] and Bitcoin [91], the network is entirely open, and anyone can join and participate in all core activities of the BC [2] such as reading data, verification and transactions execution. However, in a private BC, such as Hyperledger [92] and Ripple [93], only approved and authorised entities can participate in and control the network. This type of BC is mainly used by companies who want to benefit from BC technology without exposing its network to the public, such as banks. A consortium BC (or federated BC), such as Quorum [94] and Corda [95], is a hybrid solution (public and private BCs), where numerous organisations manage the platform. For instance, several companies that operate in the same industry can deploy a consortium BC as a single platform to conduct transactions and transmit information [1]. Table I summarizes the main characteristics of private, public and consortium BCs.

The main characteristics of BC, including integrity, immutability of the data, decentralisation, irreversibility, persistence, transparency and anonymity [13], [123], make it the most suitable solution in all fields requiring secure data sharing among multiple parties. Autonomous driving is certainly one of the important application areas of BC, where it has been considered by the research community as a potential solution for enhancing data security, integrity and transparency [2], [82], [123], [124]. In particular, the research community has applied BC and distributed ledger technologies in the following aspects of AV security and privacy.

Insert Table 1 here

1) Transparent and Secure Storage of Data: Analysts predict that AVs will soon generate significantly more data than people, with more than 4,000 GB of data per day [125]. BC, with its distributed information sharing and tamper-resistant features, can provide transparent and secure storage of the sensitive data generated by AV systems [112], [126], [127]. In this context, many studies [96], [97], [98], [128] investigated the usage of BC for distributed and secure storage of data in vehicular networking. For instance, in [13], the data that need to be distributed through the BC network has been classified into five main categories: data monitored by RSUs (e.g. speed, driving habits), in-vehicle sensory data (e.g. electronics, air pressure, temperature), vehicle insurance data, infotainment data (e.g. voice, video) and vehicle financial transactions data (e.g., refuelling, charging, washing). Thus, five different BCs were designed according to different applications in vehicular networks. The data communications of different types of BCs are independent. Similarly, authors in [98] proposed a BC-based storage architecture for decentralized and secure storage of the data generated by the AVs in the cloud layer with a

Distributed Hash Table (DHT). This architecture has been implemented with the Ethereum platform, where the primary nodes are AVs and RSU. RSU nodes are used for mining, blocks generation, and data authentication and verification.

2) Securing Communication Channels: BC as a collaborative and decentralized security technique can also make the AV communication channels (either inter-communication channel or intra-communication channel) more trustworthy, secure, reliable, and tamper-proof [13], [82], [105], [127]. Thus, a number of studies have leveraged the principles of BC in order to secure data transmission in various channels [101], [102], [105], [129], [130]. For instance, authors in [101] proposed a BC-based solution that uses the Proof of Driving (PoD) [131] consensus protocol to ensure secure and faster communications between AVs. PoD randomizes the selection of honest miners to efficiently generate the blocks. In addition, each AV is associated with a unique encrypted identifier which can be issued by the vehicle seller or an authorized authority. This number is used to improve the privacy of AVs and access their complete history. Authors in [105] proposed a BC-based framework to mitigate ECU exploitation by monitoring the state of the in-vehicle network to facilitate the detection of an ECU compromise. In [129], authors exploited the Ethereum smart contracts to securely manage inter-vehicular communications. Smart contracts also ensure that the data will not be shared without authorization. The identity of the AVs joining the BC network is approved by using a ring-signature-based scheme. Researchers [103], [132] exploited the BC technology to solve security issues related to data transmission between AVs and RSUs. In [103], authors proposed a decentralized trust management system in which the trust scores of AVs are maintained in a BC and shared between RSUs. Due to the limited processing power of AVs, RSU nodes are used for mining and blocks generation. In addition, a joint Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus mechanism is used to enable all the RSUs to participate in computing and updating the trust scores in a decentralized manner. Consortium BC and smart contracts technologies have been exploited in [132] to achieve secure data storage and sharing in vehicular edge networks. The smart contracts are used for data sharing and storage within the AVs as well as the RSUs edge nodes. In [133] BC is used to prevent 51% Attacks and ensure that malicious AVs cannot manipulate, change, or delete the critical-event messages in a VANET.

Security and privacy issues related to the AV IoT sensors have been addressed in [104] by proposing a BC-based solution, where each sensor/actuator of the AV is registered to the BC network before acquiring any of the services. For performance reasons, the authors proposed that only relevant information related to the IoT sensor is stored in the BC. Therefore, even one or more smart sensors are compromised, the AVs connected to the BC network are aware of the information registered under that compromised sensor. In [130], authors exploited the BC technology for providing autonomic, secure, and dependable AV services. The BC network is managed by a Cloud Service Provider (CSP), which provides a number of VMs representing the ride-sharing service providers and users connected to the BC platform. Due to limited capabilities, smart IoT devices are not nodes by themselves, but they are connected to the nodes of the BC network, which do the necessary computation for them. The proposed solution is implemented by using the private BC Hyperledger Fabric.

3) Data Integrity and Privacy: The immutability and decentralization features of BC make it a powerful security solution to tackle data integrity and privacy problems [127]. For that, many studies proposed to use of BC technology for increasing data integrity and privacy in the AV ecosystem [113], [114], [134]. For instance, in [113], the private BC Exonum is used for tracking the AV actions and sending the parameters of the current state of each AV through neighbouring ones. Whereas, authors in [134] discussed a VANET BC implementation to ensure data integrity and security. Similarly, authors in [135] proposed a BC-based solution for secure and tamper-resilient intra-vehicular data aggregation. IoT sensors and control units participating in the BC network will require on-board identity management modules to ensure the integrity and authenticity of the data during aggregation. In addition, a trusted execution environment is used for secure execution of the core data fusion and real-time decisions.

Insert Table 2 here

In [114], authors proposed a BC-based distributed trust and reputation model to address information integrity and data tampering threats in AVs networks. The proposed trust model is built upon some of the key tenets of the IOTA Tangle distributed ledger [136] that is specifically designed for IoT environments. Authors in [112] proposed a BC-based architecture to improve the integrity of information inside the AV, where each ECU can act as a miner and shares its information with other ECUs. ECUs that work as miners hold a copy of the BC and the CAN bus is used to broadcast all transactions and blocks. In [110], a decentralized BC-based architecture is proposed for protecting AV identity and location privacy. The proposed architecture is based on the OTChain [111], which is designed for secure authorized access to IoT resources. It is also worth mentioning the Mobility Open Blockchain Initiative (MOBI) [137], which is one of the largest consortiums that is created by several well-known vehicle manufacturers and suppliers. This group aims to preserve data integrity and privacy in connected AVs and transportation systems by creating standards in BC, distributed ledger and related technologies.

Conventional routing algorithms in mesh UAS networks are also vulnerable to cyberattacks such as black Hole attacks, where a malicious node can flood fake routing information to either disrupt the network or cause packet congestion in specific nodes. For that, many recent studies have exploited the features of BC to enable UAS in mesh networks to collect and redistribute routing information in a secure manner and avoid the disclosure of sensitive network topology in the presence of compromised nodes [34], [106], [138].

4) Forensics Applications: Blockchain technology has also been exploited for forensic purposes, where AV data is recorded on an externally shared ledger that is accessible by authorized third parties, with an aim to prevent malicious tampering and accurate auditing [105], [109], [116], [139], [140], [141], [142]. In this context, authors in [139] proposed a BC-based event recording system for accident forensics. In this work, authors designed a new dynamic federation consensus scheme, called “proof of event”, for recording and broadcasting of events. In addition, a credit score is used to measure how ‘trusted’ an AV is. This includes being a witness or a versifier to an accident. Similarly, a BC-based system for forensic analysis of traffic

accidents is proposed in [109]. The BC framework connects AVs to maintenance service providers, vehicle manufacturers, law enforcement and insurance companies. Evidence and other related data are collected and kept in a permissioned BC that uses byzantine consensus protocols. Another BC-based accident forensics architecture is proposed in [142] for improving the law violation detection in smart roads. This architecture can be used for both online (i.e., the accident is close to RSUs) and offline (i.e., the accident is far from RSUs). Table II presents recent BC-based solutions related to Avs's security and privacy.

5) Reputation and Trust Management: In order to solve the limitations of centralised trust models, many studies about vehicular trust models applied BC technology to store AV reputation information for ensuring trusted communications and mitigate adversary attacks [119], [120], [121], [122]. For instance, a consortium BC has been used in [121] to store

Insert Fig. 6 here

the transactional updates through a reputation score. Nodes with a registration score higher than a threshold are allowed to communicate messages in the V2X network. In [120], a lightweight BC is used in the in-vehicle network to store local traffic information created for one-day and is destroyed the next day, while the reputation information of the AV is recorded and managed through a global BC where the RSU is a full node.

B. Literature Review on Artificial Intelligence Models

AI is a branch of computer science, which involves concerns of developing computer programs that are capable of performing intelligent and complex tasks as humans do [88]. Recently, AI technologies have made major progress and emerged in various fields including cybersecurity, where they have proven to be extremely helpful in mitigating security as well as privacy threats in many areas [143], [144]. In particular, Machine Learning (ML), which is a specific subset of AI, has become a vital technology for cybersecurity. With ML, cybersecurity systems can find patterns in data, learn from them to help prevent similar attacks and dynamically respond to changing behaviour. This helps security mechanisms to be more proactive in preventing threats and responding to active attacks in real-time [143], [145], [146]. Motivated by these successes, researchers in the automotive industry have also applied ML techniques for behavioural analysis of the big data coming from the AV and its surrounding environment in order to identify potential attacks which can be difficult to detect with conventional cybersecurity solutions [9], [146].

As shown in Figure 6, the three categories of ML that have been widely used are supervised, unsupervised and reinforcement learning [46]. Supervised learning refers to learning by training a model on labelled data and the learning process is supervised by matching the predictions. This learning method can be applied to regression, prediction and classification problems [144], [146], [147]. Unlike supervised learning, unsupervised learning does not require labelled or tagged data, but it can find hidden relationships and patterns in a large set of data points [147], [148]. Especially in complex tasks, such as autonomous driving, this learning method can be useful to find solutions that would hardly be solvable by convolutional methods [9], [144].

Reinforcement Learning (RL) is concerned with evaluative feedback, but no supervised signals [149], [150]. In this learning method, an agent learns behaviour through trial-and-error interactions with a dynamic, uncertain and complex environment [150]. The main challenge in RL is the preparation of the simulation environment, which is highly dependent on the task to be performed [149]. In the AV cybersecurity area, various ML techniques have been successfully deployed to improve data privacy and integrity, trust management, collaborative learning and to design new Intrusion Detection Systems (IDSs) and malware analysis methods that can handle various newly arising attacks in the AV internal and external networks [56], [146], [151].

1) Intrusion Detection and Prevention: There have been many attempts to design new ML/DL-based intrusion detection techniques for securing the CAN network and VANETs. Classification techniques such as k-nearest neighbour (K-NN), support vector machine (SVM), artificial neural networks (ANN), hidden Markov model (HMM) and one-class support vector machines (OCSVM) have gained the attention of many researchers in this field. In [56], a security system to protect vehicular ad-hoc networks was proposed. This system employed the k-NN algorithm to identify malicious vehicles for external communication in autonomous and semi-autonomous vehicles. In a similar approach [152], SVM, OCSVM and standard neural network models were used for intrusion and anomaly detection within automotive CAN networks. Similarly, authors in [146] proposed a new intrusion detection method based on a modified one-class SVM in the CAN traffic by deploying three attacks (i.e., DoS, fuzzing, and spoofing attacks). In another work [173], an HMM-based detection and mitigation technique is proposed to detect attacks against Cooperative Adaptive Cruise Control (CACC) applications. Artificial neural networks (ANNs) were employed in [174] to identify the malicious behaviour in VANETs of AVs.

Deep learning (DL), which is one of the powerful ML techniques, has been also applied by many researchers to design IDS/IPSs for AVs cybersecurity [54], [175], [176]. Deep neural network (DNN), long short-term memory (LSTM), recurrent neural network (RNN), and convolutional neural network (CNN) are among the most used DL models in this field. In [176] an IDS using DNN was proposed to secure the invehicular network. In [175], LSTM was used to propose an IDS for detecting various attacks on the CAN bus network, such as DDoS, fuzzing, and spoofing attacks. LSTM was also used with RNN in [154] to identify spoofing attacks in CAN bus. A hybrid network combining CNN and LSTM models was applied in [151] to identify four types of CAN bus attacks, namely flooding, fuzzing, spoofing and replaying attacks. In a previous work [177], authors focused on detecting DDoS, command injection, and malware attacks targeting the in-vehicle network by applying recurrent deep learning (RDL) and LSTM. In a similar approach [158], authors proposed a DL-based anomaly detection model for cyberattacks detection in the in-vehicle network. The model is designed based on generative adversarial network (GAN) classification to assess the message frames transferring between the ECU and other hardware in the vehicle. In [153] authors developed an intrusion detection method for securing the in-vehicle network using the deep contractive autoencoder (DCAE) model.

Deep Transfer Learning (DTL) is also used as a solution in terms of intrusion detection. DTL can reuse previous trained-model knowledge and outperform other traditional ML and DL models. In

[156] authors proposed a deep transfer learning-based IDS model for In-Vehicle Network (IVN) along with improved performance in comparison to several other existing models. The proposed model can effectively identify and classify the normal and attack scenarios of in-vehicle networks to correctly manage vehicle communications for vehicle security. Reference [178] proposed a DTL-based intrusion detection scheme of different types of attacks for the connected AVs. In [179], an intelligent IDS model based on CNNs, TL, and ensemble learning techniques is proposed to protect AV systems. In [155], authors proposed an IDS based on Transfer Learning using Deep Belief Network (DBN) to detect the attacks in the vehicle communications channels. Their proposed model outperforms other standard ML/DL models used in the same environment, such as SVM, RNN and DNN. Recently, In [161] transfer learning using DNN models is employed to propose a solution against Adversarial Attacks in AVs.

2) Malware Analysis and Classification: In the never-ending battle against malware, many researchers in the field of AV security have applied ML/DL techniques for new malware detection due to its ability to automate the malware analysis and detection process [163]. In the area of AVs, authors in [60] proposed a ML-based malware classifier trained on multi-features using ten different learning methods including K-NN, along with Opcode N-gram and Pixel feature. The proposed method was able to classify malware to their family with an accuracy of 99.99%. In [164], authors proposed a ML-based framework for detecting new zero-day bot malware specific to the vehicular context, especially, WAVE Short Message Protocol (WSMP)-Flood and GeoWSMP Flood. The proposed solution has been tested with the ML algorithms Naive Bayes (NB), SVM, k-NN, Decision Trees (DT), Random Forest (RF), Neural Network (NN) and Multilayer perceptron (MLP). The experimental results showed that this solution outperforms existing solutions with a detection rate higher than 97%.

3) Reputation and Trust Management: Many studies have proposed dynamic reputation and trust models for securing communication of AVs by using different ML techniques [147], [148], [165], [168]. In [165], authors proposed a trust model to detect the presence of malicious vehicles in vehicular networks. This work applied the Bayesian Neural Network (BNN) to model trust as a classification process and extract relevant features that can be used for intelligent decision and effective computation of trust of honest and dishonest vehicles. Studies [147], [148], [166], and [168] applied Deep Reinforcement Learning (DRL) to design dynamic trust models for securing communication of AVs. DRL is a novel subset of ML that combines DL algorithms with RL methods (e.g., Q-learning, SARSA) in order to help software agents learn how to reach their goals [146]. In [147], authors proposed a trust-based method for limiting the wrong feedback from malicious vehicles. In this work, feedback from AVs is combined in vehicular edge computing servers and the results are used to predict the average number of true messages. The edge server then uses a DRL method that combines the Q-learning method with DNN to determine the optimum reputation update policy to stimulate vehicles to send true feedback. The authors affirmed that their trust method achieved better results in terms of the average number of true feedbacks compared to the existing reputation-based methods. Whereas, in [148], a Software-Defined Networking (SDN) controller is used as an agent to learn

the most trusted routing path by DNN in VANETs, where the trust model is designed to evaluate neighbours' behaviour of forwarding routing information.

4) Data Privacy and Integrity: Lately, there has been extensive research on the usage of Federated Learning (FL) approach to support data privacy and integrity, through the dissociation of data generated by AVs and ML model aggregation [180], [181], [182], [183]. FL is simply the decentralized form of ML, where the learning algorithm is trained across multiple decentralized edge devices or servers holding local data samples. This collaborative learning approach solves many critical issues related to data privacy and integrity, data access rights and access to heterogeneous data [180]. In traditional ML methods, if there are several data sets in a server, they could be linked and lead to privacy violation, even if a data set has been "anonymized". On the contrary, for the purposes of FL, data transmitted would consist of "minimal updates" so that the accuracy of a learning model is improved. The updates themselves could be temporary, and would not contain more information than the raw data used for training [181]. The usage of FL over ML in vehicular network applications is investigated in [182]. In this study, authors provide a comprehensive analysis on the feasibility of FL for ML-based vehicular applications, including secure data sharing in vehicular networks. In more recent work [169], authors introduced FL into autonomous driving to preserve vehicular privacy by keeping original data in a local vehicle and sharing the training model parameter only with the help of Multi-Access Edge Computing (MEC) server. The problem of malicious MEC servers and malicious vehicles has been addressed by using an auxiliary BC-based reputation system. In a similar approach [170], authors applied FL and CNN for enhancing data privacy and mitigating data leakage in the AV systems.

In more recent work [171], misbehaviour detection system is proposed by using FL for local training of the model using Basic Service Message (BSM) data generated on vehicles. BSM may include critical and private information like current speed, location, etc. Different ML and DL algorithms have been used as training algorithms including SVM, KNN, LSTM and ANN. In another work [172], RL technique has been used to preserve the privacy of the AV location information. This sensitive information can be exploited by hackers to exploit the users' preferences and life patterns. Table III presents recent AI-based solutions related to the AV's security and privacy.

Insert Table 3 here

Insert Table 4 here

C. Literature Review on the Integration of Blockchain and Artificial Intelligence

Blockchain and AI technologies have different working paradigms, as illustrated in Table IV [184], but when merged, they can empower each other, and solve security and privacy issues in various sectors [184]. In this context, some leading companies start investing in the combination of BC and AI projects in order to enhance security and data privacy in different areas. Some important projects are Engima [185], Numerai [186], SingularityNET [187], Ocean protocol [188], Synapse AI, Namahe AI [189] and Computable labs. In the context of autonomous vehicles, many recent studies have shown that the integration of BC and AI is powerful and is set to

enhance the AVs privacy and protection against cyberattacks [12], [82], [83], [88], [184], [190], [191], [192].

1) Secure Communication Channels: AI techniques can optimize the construction of the BC to make it more efficient, secure and energy-saving [82], [181], [184]. While, the main features of BC, including security, transparency, decentralization and immutability, enable AI-based solutions applied to AVs security to become more transparent, trustful and explainable [184]. In this context, the CUB platform [12], which is a recent project, integrated both BC and AI with AVs to protect the in-vehicle network and V2X communications. In this project, a hybrid BC solution is deployed by combining a public BC with their own private BC in order to provide faster and more trustful data processing, transmission, and receipt. In this work, the deep learning method stochastic gradient descent (SGD) is applied to enhance the BC processing speed. Furthermore, Deep learning and reinforcement learning models have been used to provide the CUBE BC with powerful intelligence for data processing and identification of malicious attacks on AVs. In addition, a quantum hashing cryptography solution is used to improve the security of the BC network.

Similarly, authors in [193] deployed both Deep Neural Network (DNN) and BC to address security challenges in smart vehicular networks. In this work, a public BC is used to ensure secure communication between authenticated components (e.g., AVs, RSUs, etc.) in vehicular Networks, while DNN is adopted to detect abnormal components which are victims of attacks, then update their status to invalid in the BC. This makes other components aware of invalid ones and prevents them from being associated with the compromised devices. In [145], authors integrated AI and BC into one network to effectively address driving safety and data security issues in vehicular networks. In this context, the Long short-term memory (LSTM) model is used to ensure safe self-driving by using time-series vehicular data to extract useful information. Each cluster of approved RSUs deploys a consortium BC network that uses the Byzantine Fault Tolerance-Delegated Proof of Stake (BFT-DPoS) consensus protocol in order to ensure excellent transaction throughput necessary to support real-time operations in the vehicular network. Authors confirmed that their approach maintained high prediction accuracy of 92.5% - 93.8%, compared to traditional centralized approaches.

Insert Table 5 here

2) Data Privacy and Integrity: The intersection of BC and AI will also offer the opportunity to safeguard the data generated by AVs against cyberattacks as well as access data in a decentralized manner [190], [195]. In this context, authors in [190], employed AI and BC to empower security and resist undesirable data modification in vehicular networks. In this work, data generated from the different AV components and sensors are sent to the nearest RSU for storage and processing. To securely store data and preserve the anonymity of AVs generating them, a consortium BC (BC 2.0 architecture) is deployed as the underlying network for each cluster of RSUs, which is formed by neighbouring RSUs. Blockchain 2.0, which is an extension of Blockchain 1.0, uses efficient consensus algorithms, such as Istanbul Byzantine Fault Tolerance (IBFT) [206], Selective Endorsement (SE) [207], and Raft-based Consensus

mechanisms [207], which can process a great number of transactions at higher speed rates with less power consumed. Due to the RSU's poor storage capabilities, newly received data is forwarded to the cloud for further analysis, where an RL model is used for new data patterns recognition and categorisation according to the various conditions. In another relevant study [195], BC and AI have been merged to preserve the privacy of data exchanged between AVs and RSUs. In this work, BC is used to create transparent and reliable information-sharing channels among AVs and RSUs, while AI algorithms are used to perceive the needs of the underlying AVs and predict relevant content requirements to RSUs or AVs who choose to be content providers.

3) Collaborative Learning: Many recent studies exploited BC to process the AI learning data in a distributed manner, without being restricted to a single entity data set [181], [191], [196], [208], [209]. This is a very important aspect of integrating BC and AI as it provides full control over the usage of data and learning models and therefore, solve the growing privacy concerns over sharing raw data of AV [201], [202], [210]. In this context, authors in [197] combined BC with a hierarchical FL algorithm to guarantee the security and privacy of knowledge during the sharing process. AVs learn environmental data through machine learning methods and share the learning knowledge with each other through the BC network. Furthermore, the BC-enabled framework is designed to deal with certain malicious attacks effectively. Authors confirmed that the proposed AI-based BC model effectively reduced the computation consumption compared with conventional BC systems and enhanced the learning accuracy by about 10% for MLP network and 3% for CNN network. In a similar approach [208], a BC-based collective learning solution is proposed, where each AV can share the learned local model as knowledge to improve the efficiency and accuracy of ML. The BC system, which replaces the central server, is used to make the collective learning process secure, automatic and transparent. Towards the same direction, studies [191], [192], [199] proposed a BC-based federated learning (BFL) design for privacy-aware and efficient vehicular communication networking, where local on-vehicle ML (oVML) model updates are exchanged and verified in a distributed fashion.

4) Collaborative Intrusion Detection: FL and BC were also used to design collaborative and distributed ML-based intrusion detection systems for AVs. FL has the capability to avoid sharing sensitive data directly, by training models locally at each vehicle. Whereas, BC can solve the problem of traditional centralised data training that highly depends on the robustness and trustworthiness of a central server. Authors in [201], proposed a distributed DL-based intrusion detection mechanism that offloads the training model to distributed edge devices (e.g., connected vehicles and roadside units (RSUs)), by using FL and BC. In this work, the Ethereum BC is used for storing and secure sharing of the training models. Whereas, the FL model is implemented by using DNNs and the "Syft" library. In a similar approach [202], authors introduced DL-based IDS for detecting cyberattacks in vehicular networks. The proposed system is integrated into a BC managed edge intelligence framework where the edge nodes (AVs, RSUs) collaboratively and reliably participate in the federated training of intrusion detection schema. Table V presents examples of some recent studies that exploited both BC and AI models for securing and preserving the privacy of the AV components and vehicular networks.

D. Limitations of the Proposed Solutions

From this study, it is observed that the integrated application of AI and BC in cybersecurity is currently the most popular topic for research as it provides the best way to detect and respond to potential threats in real-time. However, the concept of combining BC and AI and its application for securing the AVs ecosystem is still in its nascent phase. Most proposed solutions are in the experimental phase only, which implies we still have to wait for a while to clearly understand what opportunities the integration offers. In fact, the effectiveness of the studied approaches is still unclear and how difficult they are to be implemented, especially, with the limited capacity of the AV components to accommodate the computing demand of AI and BC techniques. Therefore, a study to validate these defence frameworks in a realistic environment is needed as most studied articles only presented theoretical frameworks that have been tested in a simple simulation environment. In this context, full-scale tests and simulations of real-world complex communication conditions are needed in order to prove the efficiency of the proposed solutions. This could be achieved through the collaboration of research projects with automotive manufacturers.

Additionally, most of the discussed articles do not take into account the various limitations of BC and AI technologies in real-world implementation such as those related to scalability, high costs, integration with legacy systems and high energy consumption. The next section presents the main limitations and challenges that should be considered when using AI and BC for securing AVs.

V. OPEN ISSUES, CHALLENGES AND FUTURE RESEARCH DIRECTIONS

In this section, we will give insights on to-date open challenges of implementing AI and Blockchain technologies in the connected AV ecosystem and some directions for researchers to take into consideration.

A. Open Research Challenges

The combination of BC technology and AI is recently considered as an efficient measure. However, both technologies within the AVs are still facing some limitations and challenges that should be addressed in future research [184], [211], [212]. Some of these foreseeable challenges are listed below:

1) Scalability and Storage: The decentralization of BC on a peer-to-peer network as well as its replication on multiple nodes provide extra security by making it more difficult for an attacker to compromise the system. However, these have a negative impact on the scalability of BC systems [213]. In fact, with the growing number of nodes and transactions, the requirement for public BC storage is also increasing, since the full nodes that store complete block data demand high storage capacity. In addition to the number of nodes and the storage, there are other factors attached to scalability that include transaction throughput, block size, high communication, latency, cost, and the verification process [59]. The increasing number of vehicles requires adding more blocks and so database size increases. For example, in smart

city applications, vehicular traces of 700 cars for 24h demand a storage capacity of close to 4.03 GB, which is about 0.24 MB per hour [59]. Thus, without completely addressing the scalability challenges, BC technology cannot reach its true disruptive potential in AVs. A number of efforts have been made to address this challenge utilizing different approaches, including the on-chain [214], the off-chain [59], parallel mining approaches [214] and software-based techniques [214]. However, this challenge still persists in AV application.

2) Performance and Computation Challenges: As can be easily understood from the data presented, the operation of AVs is already based on extremely complex interconnected systems, which require constantly fast exchanges and processing of an incredibly large volume of data [2], [9], [140]. In other words, the above-mentioned systems should perform without the slightest problem, since in any other case, e.g., an error or a delay in processing or communication, there could even be loss of human lives and physical damage. The situation described above becomes even more complicated if additional mechanisms are added to AV systems to implement BC technology and solutions based on AI techniques. More specifically, these mechanisms will require additional technological resources for faster processing and wired and wireless communications for data exchanges, always based on security and privacy, on the one hand causing performance problems in the systems, and on the other hand, rising production costs due to high resource demands and computational complexity, as explained in [208], [215], [216], and [217]. According to current research, there are solutions that are not based on BC, such as smart contracts without BC, proposed in [218]. Nevertheless, these solutions, that do not use BC, are obviously outside the scope of the current research.

3) Vulnerability: Blockchain and AI have been recently found vulnerable to several cyberattacks and a number of security issues have arisen [44], [87], [110], especially when it comes to processing sensitive data. Smart contracts and BC are vulnerable to 51% attacks, cryptojacking, Sybil attacks, whitewashing attacks, eclipse attacks, refusal-to-sign and many others. Security issues and vulnerabilities related to the usage of BC in AVs networks have been deeply investigated in [87], [127], and [181]. The future quantum computing also presents a serious threat to the crypto industry, the backbone of BC technology as quantum computers can crack the encryption of even the most advanced BCs in few seconds.

AI systems are also vulnerable to adversarial attacks, which become an inherent weakness of Ml/DL models [36], [71], [72]. Studies [21] and [219] provided a detailed description of the main vulnerabilities in AI systems. In parallel, a recent study in [220] discussed some security challenges related to the usage of AI in the AV ecosystem. Moreover, integrating both technologies will surely be compounded by new vulnerabilities and security problems. BC is based on cryptography algorithms which make data theft a complicate task. However, it is crucial to decrypt the data first, so that the AI can generate better predictions, which can lead to data breaches. In addition, successfully exploited vulnerabilities will have serious impact on the whole network.

4) Lack of Transparency and Trust in AI Systems: The application of AI models will certainly bring strong security protection for AVs; however, this technology has a key drawback that

should be considered in order to build a trusted AI-based system. In fact, most AI-based systems are perceived as a black-box that allows powerful predictions, but it cannot be directly interpreted due to the difficulties in determining how and why it makes certain decisions. Actually, lack of transparency and trust in modern AI systems poses important ethical issues as highlighted in the “ethical guidelines” published by the EU Commission’s High-Level Expert Group on AI (AI HLEG) in March 2020 [221]. Recent legislation, such as the European General Data Protection Regulation (GDPR), enshrines the right to explanation for ML decisions. In order to solve this issue, research on the explainability of AI algorithms (i.e., eXplainable Artificial Intelligence (XAI), or Interpretable AI), which represents a novel research path, is currently raising, especially in the ecosystem of AVs and their security against cyberattacks [222], [223], [224].

5) Lack of Standards and Regulations: Both Blockchain and artificial intelligence are two areas that have emerged very recently and continue to evolve rapidly. The same does not happen with the legal framework that governs their operation and their overall integration into the political, social and economic life of a country. This is a more general situation in terms of the coexistence of technology and legislation: legislation adapts very slowly to technological developments. Although there is already a great deal of discussion about the processing of personal data related to AVs [225], in fact, nationally and internationally, efforts are being made to set rules for the operation of both BC and AI. Indicatively, in [226], the authors provide up-to-date information about legal regulation of AVs in Europe and the United States of America (U.S.). At EU level, there are approaches for the AI [227], as well as for Blockchain [228]. More specifically, the EU wants to be a leader in BC technology, becoming an innovator in Blockchain and a home to significant platforms, applications and companies. At the same time, the EU’s approach to AI centres on excellence and trust, aiming to boost research and industrial capacity and ensure fundamental rights.

6) Lack of Dedicated Datasets: According to our findings, we observe that there is no well-known and widely recognized datasets dedicated for training artificial intelligence systems and assessing the effectiveness of the proposed security methods in the field of connected AVs. In addition, the limited amount of training data is a real issue for AI in these security solutions. Therefore, the research community should devote more time to collecting more specific data or building more detailed and sufficiently large sets that are collected from real-world scenarios of attacks against AVs in order to correctly assess the effectiveness of the proposed security solutions.

7) Environmental Pollution: As discussed before, Integrating BC and AI technologies with AVs requires high processing speed and power consumption, which could significantly rise the emission of greenhouse gases, increase pollution and therefore have negative impacts on climate change. In this context, Green Computing (GC) approaches, including green design, green Awareness, green usage and green standards are getting additional consideration.

B. Recommendations for Future Research Directions

The discussed challenges open several research directions related to the three paradigms, i.e., AI, Blockchain, and AVs. In this section, we discuss some important research directions.

1) Integration of Quantum Computing With Explainable AI and Blockchain: Explainable AI is a new research path that aims to create more explainable ML/DL models while maintaining a high level of learning performance (i.e., High detection accuracy rate), and enable human users to understand, trust, and effectively interpret the emerging generation of artificially intelligent partners [229]. On the other hand, Quantum technology may appear to be a viable solution to current issues relating to the performance and scalability issues of blockchain technology and AI algorithms training. Quantum computers can enhance the scalability and speed of distributed consensus (Quantum consensus) [230]. Currently, Post Quantum and Quantum BCs present a new research direction aiming to create BCs capable of resisting the threats from quantum computers by using quantum and post-quantum cryptography techniques to encrypt data. These techniques are currently a hot research topic and some research projects and initiatives have already proposed post-quantum BCs or modifications of current BCs like PQCrypto and Quantum Resistant Ledger (QRL). This new technology can be used to develop innovative solutions that will securely and privately hold data generated by AVs and withstand post-quantum computational power.

Quantum BCs with explainable AI and quantum computing can solve the discussed challenges, especially those related to security, trust, transparency, scalability and performance, and thus, move a step closer to secure smart AVs, safer, more transparent and more efficient in the near future.

2) Using Specialised Trusted Hardware Devices and Trusted Execution Environments: One of the overlooked aspects in integrating BC and AI with AVs is the impact hardware faults can have on BC execution and AI decisions. This impact is of significant importance, especially when deployed in safety-critical applications such as AVs and intelligent transportation systems. In this context, high-processing machines and Trusted Execution Environments (TEEs) are fairly new technological approaches that can solve these problems and secure data transmission as well as processing in the AV environment.

3) Usage of Computational Offloading Mechanisms: Computation offloading is a promising approach that significantly reduces overhead on AV devices and improves the mobile QoS by offloading computation tasks to a resourceful entity [231]. It can be performed as a new service paradigm in cloud-IoT ecosystem, and directly impact the scalability of the physical resources as well as the service itself [232]. Many offloading techniques have been proposed in the literature focusing on fog or edge computing in the cloud-IoT environment [232]. According to [231], offloading is being important for intelligent transportation systems and can significantly improve their performance. Vehicles frequently need to offload their tasks either partially or entirely, to more powerful entities like clouds, fogs, and cloudlets.

4) Federated Learning and BC-Based UAV Networks: The integration of federated learning with BC-based UAV networks can provide a promising security solution that fulfils the processing and storage needs at AV wide-scale networks, facilitate the distribution of generated data processing and analysis, and improve the scalability and management of massive mobile connectivity.

VI. CONCLUSION

Despite the benefits of autonomous vehicles, these network-based engines are highly susceptible to privacy and security attacks. In this article, we have elaborated on this topic by first presenting the key components of autonomous vehicles and their internal and external communication networks. This presentation has served as a baseline for a systematic review of the most critical cyberattacks on both AV components and communication channels based on the current literature and recently reported attacks. This review is concluded with a new classification of the identified cyberattacks according to their goals and proposes. In this context, several defensive techniques and countermeasures are explored. In particular, the usage of AI and BC technologies for securing connected AVs against malicious attacks has recently attracted great attention in both the academic and industrial sectors.

Both technologies can make a better combination as AI can perfectly process the huge amount of data generated by AVs and make good decisions, whereas Blockchain provides a highly secured and trusted platform for data storage and sharing through in-vehicle and V2X networks. In this article, we have reviewed the current state-of-the-art related to the usage and applicability of Blockchain, AI and both of them for preserving the AV's security and privacy. Our literature review shows that the integration of both technologies is still in its early development stage and most proposed solutions are in the experimental phase. In addition, there are many research challenges and open issues that should be addressed and tackled in areas related to security, performance, scalability, data storage, transparency, interoperability, regulation and standards. All these aspects have been discussed in this article as well as future research directions.

ACKNOWLEDGMENT

The work reflects the authors' view and the Agency is not responsible for any use that could be made from the information it contains.

REFERENCES

[1] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” Ad Hoc Netw., vol. 90, Jul. 2019, Art. no. 101823.
[2] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, “Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review,” Comput. Electr. Eng., vol. 86, Sep. 2020, Art. no. 106717.
[3] G. J. M. Read, S. Shorrock, G. H. Walker, and P. M. Salmon, “State of science: Evolving perspectives on ‘human error,”’ Ergonomics, vol. 64, no. 9, pp. 1091–1114, Sep. 2021.
[4] How Many Connected Cars Are Sold Worldwide. Verzion. Accessed: Apr. 15, 2021. [Online]. Available: https://smartcar.com/ blog/connected-cars-worldwide/
[5] A. Proch. By 2030, One in 10 Vehicles Will Be Self-Driving Globally. Statista. Accessed: Sep. 30, 2021. [Online]. Available: https://www.statista.com/press/p/autonomous_cars_2020/
[6] F. Holmes. Autonomous Cars Low on a Hacker’s Hit List, for Now. Automotive World. Accessed: Oct. 30, 2021. [Online]. Available: https://www.automotiveworld.com/articles/autonomous-cars-lowon-a-hackers-hit-list-for-now/
[7] A. Taeihagh and H. S. M. Lim, “Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks,” Transp. Rev., vol. 39, no. 1, pp. 103–128, Jul. 2018.
[8] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: Future challenges,” IEEE Trans. Intell. Transp. Syst., vol. 18, no. 11, pp. 2898–2915, Nov. 2017.
[9] M. Pham and K. Xiong, “A survey on security attacks and defense techniques for connected and autonomous vehicles,” Comput. Secur., vol. 109, Oct. 2021, Art. no. 102269.
[10] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, “Internet of autonomous vehicles communications security: Overview, issues, and directions,” IEEE Wireless Commun., vol. 26, no. 4, pp. 60–65, Aug. 2019.
[11] S. Kim, “Blockchain for a trust network among intelligent vehicles,” in Advances in Computers, vol. 111. Amsterdam, The Netherlands: Elsevier, 2018, pp. 43–68.
[12] CUBE. Cube Autonomous Car Network Security Platform Based on Blockchain. Accessed: Dec. 5, 2021. [Online]. Available: https://cubeint.io/
[13] R. Gupta et al., “VAHAK: A blockchain-based outdoor delivery scheme using UAV for healthcare 4.0 services,” in Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Jul. 2020, pp. 255–260.
[14] H.-K. Kong, T.-S. Kim, and M.-K. Hong, “A security risk assessment framework for smart car,” in Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2016, pp. 102–108.
[15] SAE International. (2019). SAE Updates J3016 Levels of Automated Driving Graphic to Reflect Evolving Standard. [Online]. Available: https://www.sae.org/news/2019/01/sae-updates-j3016-automateddriving-graphic
[16] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, “Autonomous vehicle: Security by design,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 11, pp. 7015–7029, Nov. 2021.

[17] A. Chattopadhyay and K.-Y. Lam, “Security of autonomous vehicle as a cyber-physical system,” in Proc. 7th Int. Symp. Embedded Comput. Syst. Design (ISED), Dec. 2017, pp. 1–6.
[18] J. Vargas, S. Alsweiss, O. Toker, R. Razdan, and J. Santos, “An overview of autonomous vehicles sensors and their vulnerability to weather conditions,” Sensors, vol. 21, no. 16, p. 5397, Aug. 2021.
[19] S. Wright. Autonomous Cars Generate More Than 300 Tb of Data Per Year. www.tuxera.com. Accessed: Oct. 15, 2022. [Online]. Available: https://www.tuxera.com/blog/autonomous-cars300-tb-of-data-per-year/
[20] S. Daily. (Jun. 6, 2022). Self-Driving Deep Learning With Lex Fridman. [Online]. Available: https://softwareengineeringdaily. com/2017/07/28/self-driving-deep-learning-with-lex-fridman/
[21] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, “Cybersecurity for autonomous vehicles: Review of attacks and defense,” Comput. Secur., vol. 103, Apr. 2021, Art. no. 102150.
[22] A. Martínez-Cruz, K. A. Ramírez-Gutiérrez, C. Feregrino-Uribe, and A. Morales-Reyes, “Security on in-vehicle communication protocols: Issues, challenges, and future research directions,” Comput. Commun., vol. 180, pp. 1–20, Dec. 2021.
[23] Y. Takefuji, “Connected vehicle security vulnerabilities [commentary],” IEEE Technol. Soc. Mag., vol. 37, no. 1, pp. 15–18, Mar. 2018.
[24] H. Wen, Q. A. Chen, and Z. Lin, “Plug-N-Pwned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT,” in Proc. 29th USENIX Secur. Symp. (USENIX Secur.), 2020, pp. 949–965.
[25] J. Wang, J. Liu, and N. Kato, “Networking and communications in autonomous driving: A survey,” IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1243–1274, 2nd Quart., 2019.
[26] P. Mutalik and V. C. Patil, “A survey on vehicular ad-hoc network [VANET’s] protocols for improving safety in urban cities,” in Proc. Int. Conf. Smart Technol. Smart Nation (SmartTechCon), Aug. 2017, pp. 840–845.
[27] H. Zhou, W. Xu, J. Chen, and W. Wang, “Evolutionary V2X technologies toward the Internet of Vehicles: Challenges and opportunities,” Proc. IEEE, vol. 108, no. 2, pp. 308–323, Feb. 2020.
[28] S. Gyawali, S. Xu, Y. Qian, and R. Q. Hu, “Challenges and solutions for cellular based V2X communications,” IEEE Commun. Surveys Tuts., vol. 23, no. 1, pp. 222–255, 1st Quart., 2021.
[29] 3GPP. (2017). Release 14. [Online]. Available: https://www. 3gpp.org/release-14
[30] GSMA. (2017). Cellular Vehicle-to-Everything (C-V2X) Enabling Intelligent Transport. [Online]. Available: https://www.gsma. com/iot/wp-content/uploads/2017/12/C-2VX-Enabling-IntelligentTransport_2.pdf
[31] 5GAA. Exploring the Technology: C-V2X. [Online]. Available: https://5gaa.org/5g-technology/c-v2x/
[32] 3GPP. (2020). Release 16. [Online]. Available: https://www. 3gpp.org/release-16
[33] O. Kavas-Torris, S. Y. Gelbal, M. R. Cantas, B. Aksun-Guvenc, and L. Guvenc, “V2X communication between connected and automated vehicles (CAVs) and unmanned aerial vehicles (UAVs),” 2021, arXiv:2109.00145.
[34] J. Wang, Y. Liu, and H. Song, “Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends,” IEEE Aerosp. Electron. Syst. Mag., vol. 36, no. 3, pp. 4–29, Mar. 2021.
[35] X. Sun, F. R. Yu, and P. Zhang, “A survey on cyber-security of connected and autonomous vehicles (CAVs),” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[36] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei, and R. Das, “Attacks on self-driving cars and their countermeasures: A survey,” IEEE Access, vol. 8, pp. 207308–207342, 2020.
[37] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, “Connected and autonomous vehicles: A cyber-risk classification framework,” Transp. Res. A, Policy Pract., vol. 124, pp. 523–536, Jun. 2019.
[38] M. C. Chow, M. Ma, and Z. Pan, “Attack models and countermeasures for autonomous vehicles,” in Intelligent Technologies for Internet of Vehicles. Cham, Switzerland: Springer, 2021, pp. 375–401.
[39] Y. Cao et al., “Adversarial sensor attack on LiDAR-based perception in autonomous driving,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Nov. 2019, pp. 2267–2281.
[40] M. El-Said, X. Wang, S. Mansour, and A. Kalafut, “Building an impersonation attack and defense testbed for vehicle to vehicle systems,” in Proc. 22st Annu. Conf. Inf. Technol. Educ., Oct. 2021, pp. 65–66.
[41] M. Baza et al., “Detecting sybil attacks using proofs of work and location in VANETs,” IEEE Trans. Depend. Secure Comput., vol. 19, no. 1, pp. 39–53, Jan. 2022.
[42] L. Christensen and D. Dannberg, “Ethical hacking of IoT devices: OBD-II dongles,” KTH, School Elect. Eng. Comput. Sci., Stockholm, Sweden, Tech. Rep. 2019:214, 2019.
[43] L. Yu, J. Deng, R. R. Brooks, and S. B. Yun, “Automobile ECU design to avoid data tampering,” in Proc. 10th Annu. Cyber Inf. Secur. Res. Conf., Apr. 2015, pp. 1–4.
[44] N. Pitropakis, E. Panaousis, T. Giannetsos, E. Anastasiadis, and G. Loukas, “A taxonomy and survey of attacks against machine learning,” Comput. Sci. Rev., vol. 34, Nov. 2019, Art. no. 100199.
[45] W. Wang, Y. Yao, X. Liu, X. Li, P. Hao, and T. Zhu, “I can see the light: Attacks on autonomous vehicles using invisible lights,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Nov. 2021, pp. 1930–1944.
[46] M. Dibaei et al., “Attacks and defences on intelligent connected vehicles: A survey,” Digit. Commun. Netw., vol. 6, no. 4, pp. 399–421, Nov. 2020.
[47] H. S. Sanchez, D. Rotondo, V. Puig, T. Escobet, and J. Quevedo, “Detection of replay attacks in autonomous vehicles using a bank of QPV observers,” in Proc. 29th Medit. Conf. Control Autom. (MED), Jun. 2021, pp. 1149–1154.
[48] R. Komissarov and A. Wool, “Spoofing attacks against vehicular FMCW radar,” 2021, arXiv:2104.13318.
[49] Y. Cao, J. Ma, K. Fu, R. Sara, and M. Mao, “Automated tracking system for LiDAR spoofing attacks on moving targets,” in Proc. Workshop Automot. Auto. Vehicle Secur. (AutoSec), 2021, p. 1.
[50] J. Patel, M. L. Das, and S. Nandi, “On the security of remote key less entry for vehicles,” in Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS), Dec. 2018, pp. 1–6.
[51] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN bus security challenges,” Sensors, vol. 20, no. 8, p. 2364, Apr. 2020.
[52] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, “A stealth, selective, link-layer denial-of-service attack against automotive networks,” in Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment. Cham, Switzerland: Springer, 2017, pp. 185–206.

[53] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, “Congestion attacks to autonomous cars using vehicular botnets,” in Proc. Workshop Secur. Emerg. Netw. Technol., 2015, pp. 1–9.
[54] C. Yan, W. Xu, and J. Liu, “Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle,” DEF CON, vol. 24, p. 109, Aug. 2016.
[55] A. Gruebler, K. D. McDonald-Maier, and K. M. A. Alheeti, “An intrusion detection system against black hole attacks on the communication network of self-driving cars,” in Proc. 6th Int. Conf. Emerg. Secur. Technol. (EST), Sep. 2015, pp. 86–91.
[56] K. M. A. Alheeti and K. McDonald-Maier, “An intelligent security system for autonomous cars based on infrared sensors,” in Proc. 23rd Int. Conf. Autom. Comput. (ICAC), Sep. 2017, pp. 1–5.
[57] N. Aleisa and K. Renaud, “Privacy of the Internet of Things: A systematic literature review,” in Proc. 50th Hawaii Int. Conf. Syst. Sci., 2017, pp. 5947–5956.
[58] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR,” Black Hat Eur., vol. 11, p. 995, Nov. 2015.
[59] D. Khan, L. T. Jung, and M. A. Hashmani, “Systematic literature review of challenges in blockchain scalability,” Appl. Sci., vol. 11, no. 20, p. 9372, Oct. 2021.
[60] X. Han, F. Jin, R. Wang, S. Wang, and Y. Yuan, “Classification of malware for self-driving systems,” Neurocomputing, vol. 428, pp. 352–360, Mar. 2021.
[61] 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.
[62] A. Al-Sabaawi, K. Al-Dulaimi, E. Foo, and M. Alazab, “Addressing malware attacks on connected and autonomous vehicles: Recent techniques and challenges,” in Malware Analysis Using Artificial Intelligence and Deep Learning. Cham, Switzerland: Springer, 2021, pp. 97–119.
[63] S. Checkoway et al., “Comprehensive experimental analyses of automotive attack surfaces,” in Proc. USENIX Secur. Symp., vol. 4. San Francisco, CA, USA, 2011, p. 2021.
[64] S. Ornes. (2022). How to Hack a Self-Driving Car. Accessed: Jan. 1, 2022. [Online]. Available: https://physicsworld.com/a/how-tohack-a-self-driving-car/
[65] F. Siddiqui. Hackers Said They Could Steal a Tesla Model X in Minutes. Tesla Pushed Out a Fix. Accessed: Jan. 1, 2022. [Online]. Available: https://www.washingtonpost.com/technology/2020/11/23/tesla-modelxhack/
[66] D. T. Le, K. Q. Dang, Q. L. T. Nguyen, S. Alhelaly, and A. Muthanna, “A behavior-based malware spreading model for vehicle-to-vehicle communications in VANET networks,” Electronics, vol. 10, no. 19, p. 2403, Oct. 2021.
[67] M. T. Garip, P. Reiher, and M. Gerla, “BOTVEILLANCE: A vehicular botnet surveillance attack against pseudonymous systems in VANETs,” in Proc. 11th IFIP Wireless Mobile Netw. Conf. (WMNC), Sep. 2018, pp. 1–8.
[68] G. Bendiab, S. Shiaeles, and N. Savage, “Malware detection and mitigation,” in Cyber-Security Threats, Actors, and Dynamic Mitigation. Boca Raton, FL, USA: CRC Press, 2021, pp. 199–246.
[69] P. Bajpai, R. Enbody, and B. H. C. Cheng, “Ransomware targeting automobiles,” in Proc. 2nd ACM Workshop Automot. Aerial Vehicle Secur., Mar. 2020, pp. 23–29.

[70] C. Brook. Chonda Shut Down Plant Impacted by Wannacry. Accessed: Dec. 25, 2021. [Online]. Available: https://threatpost.com/honda-shutdown-plant-impacted-by-wannacry/126429/
[71] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, “Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward,” IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 998–1026, 2nd Quart., 2020.
[72] Y. Wang, E. Sarkar, M. Maniatakos, and S. E. Jabari, “Watch your back: Backdoor attacks in deep reinforcement learning-based autonomous vehicle control systems,” Work, vol. 8, no. 28, p. 12, 2020.
[73] G. F. Elsayed, I. Goodfellow, and J. Sohl-Dickstein, “Adversarial reprogramming of neural networks,” 2018, arXiv:1806.11146.
[74] N. Akhtar and A. Mian, “Threat of adversarial attacks on deep learning in computer vision: A survey,” IEEE Access, vol. 6, pp. 14410–14430, 2018.
[75] C. Sitawarin, A. N. Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, “DARTS: Deceiving autonomous cars with toxic signs,” 2018, arXiv:1802.06430.
[76] Kaspersky. Hackers Could Use Mobile Apps to Steal Connected Cars, Says Kaspersky. Accessed: Jan. 11, 2022. [Online]. Available: https://internetofbusiness.com/hackers-connected-cars-kaspersky/
[77] L. Collingwood, “Privacy implications and liability issues of autonomous vehicles,” Inf. Commun. Technol. Law, vol. 26, no. 1, pp. 32–45, Jan. 2017.
[78] H. Lim and A. Taeihagh, “Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications,” Energies, vol. 11, no. 5, p. 1062, Apr. 2018.
[79] E. G. Abdallah, M. Zulkernine, Y. X. Gu, and C. Liem, “Towards defending connected vehicles against attacks,” in Proc. 5th Eur. Conf. Eng. Comput.-Based Syst., Aug. 2017, pp. 1–9.
[80] C. Bernardini, M. R. Asghar, and B. Crispo, “Security and privacy in vehicular communications: Challenges and opportunities,” Veh. Commun., vol. 10, pp. 13–28, Oct. 2017.
[81] M. S. Sheikh, J. Liang, and W. Wang, “Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey,” Wireless Commun. Mobile Comput., vol. 2020, pp. 1–25, Jan. 2020.
[82] M. Dibaei et al., “Investigating the prospect of leveraging blockchain and machine learning to secure vehicular networks: A survey,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 2, pp. 683–700, Feb. 2022.
[83] D. Reebadiya, T. Rathod, R. Gupta, S. Tanwar, and N. Kumar, “Blockchain-based secure and intelligent sensing scheme for autonomous vehicles activity tracking beyond 5G networks,” Peer Peer Netw. Appl., vol. 14, pp. 2757–2774, Feb. 2021.
[84] M. Obaidat, M. Khodjaeva, J. Holst, and M. B. Zid, “Security and privacy challenges in vehicular ad hoc networks,” in Connected Vehicles Internet Things. Cham, Switzerland: Springer, 2020, pp. 223–251.
[85] I. A. Sumra et al., “Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET),” in Proc. 3rd Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT), Oct. 2011, pp. 1–8.

[86] T. Hoppe, S. Kiltz, and J. Dittmann, “Security threats to automotive CAN networks-practical examples and selected short-term countermeasures,” Rel. Eng. Syst. Saf., vol. 96, no. 1, pp. 11–25, 2011.
[87] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, “On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance,” Comput. Netw., vol. 191, May 2021, Art. no. 108005.
[88] Z. Zhang, X. Song, L. Liu, J. Yin, Y. Wang, and D. Lan, “Recent advances in blockchain and artificial intelligence integration: Feasibility analysis, research issues, applications, challenges, and future work,” Secur. Commun. Netw., vol. 2021, pp. 1–15, Jun. 2021.
[89] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, pp. 1–32, Apr. 2014.
[90] Litecoin. Litecoin Foundation. Accessed: Sep. 29, 2021. [Online]. Available: https://litecoin.org
[91] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Decentralized Bus. Rev., 2008.
[92] Hyperledger Fabric Documentation. Accessed: Dec. 5, 2021. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release2.0/whatsnew.html
[93] Ripple. (2020). Ripple Documentation. Accessed: Dec. 5, 2021. [Online]. Available: https://ripple.com/xrp
[94] Quorum. (2020). Quorum Documentation. Accessed: Dec. 5, 2021. [Online]. Available: http://docs.goquorum.com/en/latest/
[95] R3. R3 Primer Series 1. Accessed: Dec. 5, 2021. [Online]. Available: https://www.r3.com/wp-content/uploads/2019/01/R3-Quick-Facts.pdf
[96] T. G. Jiang, H. Fang, and H. Wang, “Blockchain-based Internet of Vehicles: Distributed network architecture and performance analysis,” IEEE Internet Things J., vol. 6, no. 3, pp. 4640–4649, Jun. 2019.
[97] X. Zhang and X. Chen, “Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network,” IEEE Access, vol. 7, pp. 58241–58254, 2019.
[98] S. K. Singh, J. H. Park, P. K. Sharma, and Y. Pan, “BIIoVT: Blockchain-based secure storage architecture for intelligent Internet of vehicular things,” IEEE Consum. Electron. Mag., vol. 11, no. 6, pp. 75–82, Nov. 2022.
[99] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, and R. Sharma, “Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G,” J. Inf. Secur. Appl., vol. 67, Jun. 2022, Art. no. 103179.
[100] M. M. Nair and A. K. Tyagi, “Preserving privacy using blockchain technology in autonomous vehicles,” in Proc. Int. Conf. Netw. Secur. Blockchain Technol. Cham, Switzerland: Springer, 2022, pp. 237–248.
[101] M. Singh and S. Kim, “Introduce reward-based intelligent vehicles communication using blockchain,” in Proc. Int. SoC Design Conf. (ISOCC), Nov. 2017, pp. 15–16.
[102] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, “Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels,” 2017, arXiv:1704.02553.

[103] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchainbased decentralized trust management in vehicular networks,” IEEE Internet Things J., vol. 6, no. 2, pp. 1495–1505, Apr. 2019.
[104] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, “A blockchain framework for securing connected and autonomous vehicles,” Sensors, vol. 19, no. 14, p. 3165, Jul. 2019.
[105] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, “B-FERL: Blockchain based framework for securing smart vehicles,” Inf. Process. Manage., vol. 58, no. 1, Jan. 2021, Art. no. 102426.
[106] J. Wang, Y. Liu, S. Niu, and H. Song, “Lightweight blockchain assisted secure routing of swarm UAS networking,” Comput. Commun., vol. 165, pp. 131–140, Jan. 2021.
[107] M. Kamal, G. Srivastava, and M. Tariq, “Blockchain-based lightweight and secured V2 V communication in the Internet of Vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 3997–4004, Jul. 2021.
[108] A. Ali, M. M. Iqbal, S. Jabbar, M. N. Asghar, U. Raza, and F. Al-Turjman, “VABLOCK: A blockchain-based secure communication in V2 V network using ICN network support technology,” Microprocessors Microsyst., vol. 93, Sep. 2022, Art. no. 104569.
[109] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, “Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles,” IEEE Commun. Mag., vol. 56, no. 10, pp. 50–57, Oct. 2018.
[110] C. Li and B. Palanisamy, “Privacy in Internet of Things: From principles to technologies,” IEEE Internet Things J., vol. 6, no. 1, pp. 488–505, Aug. 2019.
[111] O. Alphand et al., “IoTChain: A blockchain security architecture for the Internet of Things,” in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2018, pp. 1–6.
[112] L. Davi, D. Hatebur, M. Heisel, and R. Wirtz, “Combining safety and security in autonomous cars using blockchain technologies,” in Proc. Int. Conf. Comput. Saf., Rel., Secur. Cham, Switzerland: Springer, 2019, pp. 223–234.
[113] S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova, and A. Pashkevich, “Blockchain technology on the way of autonomous vehicles development,” Transp. Res. Proc., vol. 44, pp. 168–175, Jan. 2020.
[114] H. Rathore, A. Samant, and M. Jadliwala, “TangleCV: A distributed ledger technique for secure message sharing in connected vehicles,” ACM Trans. Cyber-Phys. Syst., vol. 5, no. 1, pp. 1–25, Jan. 2021.
[115] S. Jha, N. Jha, D. Prashar, S. Ahmad, B. Alouffi, and A. Alharbi, “Integrated IoT-based secure and efficient key management framework using hashgraphs for autonomous vehicles to ensure road safety,” Sensors, vol. 22, no. 7, p. 2529, Mar. 2022.
[116] M. Li, Y. Chen, C. Lal, M. Conti, M. Alazab, and D. Hu, “Eunomia: Anonymous and secure vehicular digital forensics based on blockchain,” IEEE Trans. Depend. Secure Comput., early access, Nov. 25, 2021, doi: 10.1109/TDSC.2021.3130583.
[117] Q. Yao, T. Li, C. Yan, and Z. Deng, “Accident responsibility identification model for Internet of Vehicles based on lightweight blockchain,” Comput. Intell., May 2022, doi: 10.1111/coin.12529.

[118] J. Kang, Z. Xiong, D. Ye, D. I. Kim, J. Zhao, and D. Niyato, “Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory,” IEEE Trans. Veh. Technol., vol. 68, no. 3, pp. 2906–2920, Mar. 2019.
[119] S. Abbes and S. Rekhis, “A blockchain-based solution for reputation management in IoV,” in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2021, pp. 1129–1134.
[120] C. Pu, “A novel blockchain-based trust management scheme for vehicular networks,” in Proc. Wireless Telecommun. Symp. (WTS), Apr. 2021, pp. 1–6.
[121] P. Bhattacharya, A. Shukla, S. Tanwar, N. Kumar, and R. Sharma, “6Blocks: 6G-enabled trust management scheme for decentralized autonomous vehicles,” Comput. Commun., vol. 191, pp. 53–68, Jul. 2022.
[122] D. Kianersi, S. Uppalapati, A. Bansal, and J. Straub, “Evaluation of a reputation management technique for autonomous vehicles,” Future Internet, vol. 14, no. 2, p. 31, Jan. 2022.
[123] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, and L. H. Koh, “Blockchain for the Internet of Vehicles towards intelligent transportation systems: A survey,” IEEE Internet Things J., vol. 8, no. 6, pp. 4157–4185, Mar. 2021.
[124] T. Dargahi, H. Ahmadvand, M. Alraja, and C. Yu, “Integration of blockchain with connected and autonomous vehicles: Vision,” Technology, vol. 26, no. 28, pp. 33–50, 2021.
[125] B. Krzanich. (2021). Data is the New Oil in the Future of Automated Driving. [Online]. Available: https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/#gs.htm2ps
[126] P. K. Sharma, N. Kumar, and J. H. Park, “Blockchain-based distributed framework for automotive industry in a smart city,” IEEE Trans. Ind. Informat., vol. 15, no. 7, pp. 4197–4205, Jul. 2019.
[127] N. Kamble, R. Gala, R. Vijayaraghavan, E. Shukla, and D. Patel, “Using blockchain in autonomous vehicles,” in Artificial Intelligence and Blockchain for Future Cybersecurity Applications. Cham, Switzerland: Springer, 2021, pp. 285–305.
[128] Y. Yin, Y. Li, B. Ye, T. Liang, and Y. Li, “A blockchain-based incremental update supported data storage system for intelligent vehicles,” IEEE Trans. Veh. Technol., vol. 70, no. 5, pp. 4880–4893, May 2021.
[129] J. A. L. Calvo and R. Mathar, “Secure blockchain-based communication scheme for connected vehicles,” in Proc. Eur. Conf. Netw. Commun. (EuCNC), Jun. 2018, pp. 347–351.
[130] M. G. M. M. Hasan, A. Datta, M. A. Rahman, and H. Shahriar, “Chained of things: A secure and dependable design of autonomous vehicle services,” in Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC), Jul. 2018, pp. 498–503.
[131] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, “Towards secure and practical consensus for blockchain based VANET,” Inf. Sci., vol. 545, pp. 170–187, Feb. 2021.
[132] J. Kang et al., “Blockchain for secure and efficient data sharing in vehicular edge computing and networks,” IEEE Internet Things J., vol. 6, no. 3, pp. 4660–4670, Jun. 2019.
[133] R. Shrestha and S. Y. Nam, “Regional blockchain for vehicular networks to prevent 51% attacks,” IEEE Access, vol. 7, pp. 95033–95045, 2019.
[134] R. Barber, “Autonomous vehicle communication using blockchain,” M.S. thesis, Dept. Comput. Inf. Sci., Univ. Mississippi, Honors, Oxford, MS, USA, 2018.

[135] S. Mitra, S. Bose, S. S. Gupta, and A. Chattopadhyay, “Secure and tamper-resilient distributed ledger for data aggregation in autonomous vehicles,” in Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS), Oct. 2018, pp. 548–551.
[136] IOTA. IOTA Tangle Distributed Ledger. Accessed: Jan. 8, 2022. [Online]. Available: https://www.iota.org/
[137] MOBI. Jbuilding the New Economy of Movement. Accessed: Jan. 14, 2022. [Online]. Available: https://dlt.mobi/
[138] Y. Liu, J. Wang, H. Song, J. Li, and J. Yuan, “Blockchain-based secure routing strategy for airborne mesh networks,” in Proc. IEEE Int. Conf. Ind. Internet (ICII), Nov. 2019, pp. 56–61.
[139] H. Guo, E. Meamari, and C.-C. Shen, “Blockchain-inspired event recording system for autonomous vehicles,” in Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN), Aug. 2018, pp. 218–222.
[140] M. Safwat, A. Elgammal, W. Badawy, and M. A. Azer, “Vehicular networks applications based on blockchain framework,” in Enabling Machine Learning Applications in Data Science. Cham, Switzerland: Springer, 2021, pp. 389–401.
[141] M. Pourvahab and G. Ekbatanifard, “Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology,” IEEE Access, vol. 7, pp. 153349–153364, 2019.
[142] V. Davydov and S. Bezzateev, “Accident detection in Internet of Vehicles using blockchain technology,” in Proc. Int. Conf. Inf. Netw. (ICOIN), Jan. 2020, pp. 766–771.
[143] M. Abbasi, A. Shahraki, and A. Taherkordi, “Deep learning for network traffic monitoring and analysis (NTMA): A survey,” Comput. Commun., vol. 170, pp. 19–41, Mar. 2021.
[144] Y. Xin et al., “Machine learning and deep learning methods for cybersecurity,” IEEE Access, vol. 6, pp. 35365–35381, 2018.
[145] L. Xia, Y. Sun, R. Swash, L. Mohjazi, L. Zhang, and M. A. Imran, “Smart and secure CAV networks empowered by AI-enabled blockchain: The next frontier for intelligent safe driving assessment,” 2021, arXiv:2104.04572.
[146] O. Avatefipour et al., “An intelligent secured framework for cyberattack detection in electric vehicles’ CAN bus using machine learning,” IEEE Access, vol. 7, pp. 127580–127592, 2019.
[147] S. Gyawali, Y. Qian, and R. Hu, “Deep reinforcement learning based dynamic reputation policy in 5G based vehicular communication networks,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 6136–6146, Jun. 2021.
[148] D. Zhang, F. R. Yu, R. Yang, and H. Tang, “A deep reinforcement learning-based trust management scheme for software-defined vehicular networks,” in Proc. 8th ACM Symp. Design Anal. Intell. Veh. Netw. Appl., Oct. 2018, pp. 1–7.
[149] R. S. Sutton and A. G. Barto, Introduction to Reinforcement Learning. Edmonton, AB, Canada: Reinforcement Learning and Artificial Intelligence Laboratory, 1998.
[150] L. P. Kaelbling, M. L. Littman, and A. W. Moore, “Reinforcement learning: A survey,” J. Artif. Intell. Res., vol. 4, no. 1, pp. 237–285, Jan. 1996.
[151] T. H. Aldhyani and H. Alkahtani, “Attacks to automatous vehicles: A deep learning algorithm for cybersecurity,” Sensors, vol. 22, no. 1, p. 360, 2022.
[152] I. Berger, R. Rieke, M. Kolomeets, A. Chechulin, and I. Kotenko, “Comparative study of machine learning methods for in-vehicle intrusion detection,” in Computer Security. Cham, Switzerland: Springer, 2018, pp. 85–101.

[153] S. F. Lokman, A. T. Othman, S. Musa, and M. H. A. Bakar, “Deep contractive autoencoder-based anomaly detection for in-vehicle controller area network (can),” in Progress in Engineering Technology. Cham, Switzerland: Springer, 2019, pp. 195–205.
[154] Y. Yang, Z. Duan, and M. Tehranipoor, “Identify a spoofing attack on an in-vehicle CAN bus based on the deep features of an ECU fingerprint signal,” Smart Cities, vol. 3, no. 1, pp. 17–30, Jan. 2020.
[155] Y. Otoum and A. Nayak, “Signature-over-the-air with transfer learning IDS for intelligent connected vehicles (ICV),” in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2021, pp. 1–6.
[156] S. T. Mehedi, A. Anwar, Z. Rahman, and K. Ahmed, “Deep transfer learning based intrusion detection system for electric vehicular networks,” Sensors, vol. 21, no. 14, p. 4736, Jul. 2021.
[157] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, “Securing smart vehicles from relay attacks using machine learning,” J. Supercomput., vol. 76, no. 4, pp. 2665–2682, Apr. 2020.
[158] A. Kavousi-Fard, M. Dabbaghjamanesh, T. Jin, W. Su, and M. Roustaei, “An evolutionary deep learning-based anomaly detection model for securing vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4478–4486, Jul. 2021.
[159] H. Al-Khateeb et al., “Proactive threat detection for connected cars using recursive Bayesian estimation,” IEEE Sensors J., vol. 18, no. 12, pp. 4822–4831, Jun. 2018.
[160] A. Kashyap, A. Chakravarthy, and P. P. Menon, “Detection of cyber-attacks in automotive traffic using macroscopic models and Gaussian processes,” IEEE Control Syst. Lett., vol. 6, pp. 1688–1693, 2022.
[161] Z. Khan, M. Chowdhury, and S. M. Khan, “A hybrid defense method against adversarial attacks on traffic sign classifiers in autonomous vehicles,” TechRxiv, pp. 1–14, Feb. 2022. [Online]. Available: https://www.techrxiv.org, doi: 10.36227/techrxiv.19071824.v1.
[162] L. Zhang and D. Ma, “A hybrid approach toward efficient and accurate intrusion detection for in-vehicle networks,” IEEE Access, vol. 10, pp. 10852–10866, 2022.
[163] C. Catal, H. Gunduz, and A. Ozcan, “Malware detection based on graph attention networks for intelligent transportation systems,” Electronics, vol. 10, no. 20, p. 2534, Oct. 2021.
[164] R. Rahal, A. A. Korba, N. Ghoualmi-Zine, Y. Challal, and M. Y. Ghamri-Doudane, “AntibotV: A multilevel behaviour-based framework for botnets detection in vehicular net
[165] E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, and L. M. S. Jaimes, “Malicious node detection in vehicular ad-hoc network using machine learning and deep learning,” in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2018, pp. 1–6.
[166] G. Karmakar, A. Chowdhury, R. Das, J. Kamruzzaman, and S. Islam, “Assessing trust level of a driverless car using deep learning,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 4457–4466, Jul. 2021.
[167] H. Mankodiya, M. S. Obaidat, R. Gupta, and S. Tanwar, “XAI-AV: Explainable artificial intelligence for trust management in autonomous vehicles,” in Proc. Int. Conf. Commun., Comput., Cybersecur., Informat. (CCCI), Oct. 2021, pp. 1–5.
[168] D. Zhang, F. R. Yu, R. Yang, and L. Zhu, “Software-defined vehicular networks with trust management: A deep reinforcement learning approach,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 2, pp. 1400–1414, Feb. 2022.

[169] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, “Privacy-preserved federated learning for autonomous driving,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 8423–8434, Jul. 2022.
[170] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, “Federated learning for data privacy preservation in vehicular cyber-physical systems,” IEEE Netw., vol. 34, no. 3, pp. 50–56, May 2020.
[171] A. Uprety, D. B. Rawat, and J. Li, “Privacy preserving misbehavior detection in IoV using federated machine learning,” in Proc. IEEE 18th Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2021, pp. 1–6.
[172] M. Min, W. Wang, L. Xiao, Y. Xiao, and Z. Han, “Reinforcement learning-based sensitive semantic location privacy protection for VANETs,” China Commun., vol. 18, no. 6, pp. 244–260, 2021.
[173] M. Jagielski, N. Jones, C.-W. Lin, C. Nita-Rotaru, and S. Shiraishi, “Threat detection for collaborative adaptive cruise control in connected cars,” in Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw., Jun. 2018, pp. 184–189.
[174] K. M. Ali Alheeti and K. McDonald-Maier, “Intelligent intrusion detection in external communication systems for autonomous vehicles,” Syst. Sci. Control Eng., vol. 6, no. 1, pp. 48–56, Jan. 2018.
[175] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, “LSTM-based intrusion detection system for in-vehicle can bus communications,” IEEE Access, vol. 8, pp. 185489–185502, 2020.
[176] M.-J. Kang and J.-W. Kang, “Intrusion detection system using deep neural network for in-vehicle network security,” PLoS ONE, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.
[177] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, “Cloud-based cyber-physical intrusion detection for vehicles using deep learning,” IEEE Access, vol. 6, pp. 3491–3508, 2018.
[178] X. Li, Z. Hu, M. Xu, Y. Wang, and J. Ma, “Transfer learning based intrusion detection scheme for Internet of Vehicles,” Inf. Sci., vol. 547, pp. 119–135, Feb. 2021.
[179] L. Yang and A. Shami, “A transfer learning and optimized CNN based intrusion detection system for Internet of Vehicles,” 2022, arXiv:2201.11812.
[180] T. Zeng, O. Semiari, M. Chen, W. Saad, and M. Bennis, “Federated learning on the road: Autonomous controller design for connected and autonomous vehicles,” 2021, arXiv:2102.03401.
[181] S. R. Pokhrel and J. Choi, “Federated learning with blockchain for autonomous vehicles: Analysis and design challenges,” IEEE Trans. Commun., vol. 68, no. 8, pp. 4734–4746, Aug. 2020.
[182] A. M. Elbir, B. Soner, S. Coleri, D. Gunduz, and M. Bennis, “Federated learning in vehicular networks,” 2020, arXiv:2006.01412.
[183] U. Majeed, L. U. Khan, A. Yousafzai, Z. Han, B. J. Park, and C. S. Hong, “ST-BFL: A structured transparency empowered cross-silo federated learning on the blockchain framework,” IEEE Access, vol. 9, pp. 155634–155650, 2021.
[184] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, “Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city,” Sustain. Cities Soc., vol. 63, Dec. 2020, Art. no. 102364.

[185] Enigma. Enigma is Securing the Future of the Web. Accessed: Jan. 14, 2022. [Online]. Available: https://www.enigma.co/
[186] NUMERAI. The Hardest Data Science Tournament on the Planet. Accessed: Jan. 14, 2022. [Online]. Available: https://numer.ai/
[187] SINGULARITYNET. The Hardest Data Science Tournament on the Planet. Accessed: Jan. 14, 2022. [Online]. Available: https:// singularitynet.io/
[188] OCEANPROTOCOL. The Hardest Data Science Tournament on the Planet. Accessed: Jan. 14, 2022. [Online]. Available: https:// oceanprotocol.com/about
[189] O. Padilla. Namahe-the First Revolutionary Blockchain AI Solution for a Transparent & Sustainable Future. Accessed: Jan. 14, 2022. [Online]. Available: https://www.linkedin.com/pulse/namahe-first-revolutionaryblockchain-ai-solution-future-padilla
[190] A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, and J. Bentahar, “AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions,” IEEE Internet Things Mag., vol. 3, no. 2, pp. 68–73, Jun. 2020.
[191] S. R. Pokhrel and J. Choi, “A decentralized federated learning approach for connected autonomous vehicles,” in Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW), Apr. 2020, pp. 1–6.
[192] L. Barbieri, S. Savazzi, M. Brambilla, and M. Nicoli, “Decentralized federated learning for extended sensing in 6G connected vehicles,” Veh. Commun., vol. 33, Jan. 2022, Art. no. 100396.
[193] E. Rabieinejad, A. Yazdinejad, A. Dehghantanha, R. M. Parizi, and G. Srivastava, “Secure AI and blockchain-enabled framework in smart vehicular networks,” in Proc. IEEE Globecom Workshops (GC Wkshps), Dec. 2021, pp. 1–6.
[194] G. Raja, K. Kottursamy, K. Dev, R. Narayanan, A. Raja, and K. B. V. Karthik, “Blockchain-integrated multiagent deep reinforcement learning for securing cooperative adaptive cruise control,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 7, pp. 9630–9639, Jul. 2022.
[195] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, “Blockchain-based privacy-aware content caching in cognitive Internet of Vehicles,” IEEE Netw., vol. 34, no. 2, pp. 46–51, Mar. 2020.
[196] S. K. Lo et al., “Towards trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems,” IEEE Internet Things J., early access, Jan. 19, 2022, doi: 10.1109/JIOT.2022.3144450.
[197] H. Chai, S. Leng, Y. Chen, and K. Zhang, “A hierarchical blockchainenabled federated learning algorithm for knowledge sharing in internet of vehicles,” IEEE Trans. Intell. Transp. Syst., vol. 22, no. 7, pp. 3975–3986, Jul. 2021.
[198] D. Zhang, W. Shi, M. St-Hilaire, and R. Yang, “Multiaccess edge integrated networking for Internet of Vehicles: A blockchain-based deep compressed cooperative learning approach,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 11, pp. 21593–21607, Nov. 2022.
[199] P. K. Sharma, D. Vohra, and S. Rathore, “Security and privacy in V2X communications: How can collaborative learning improve cybersecurity?” IEEE Netw., vol. 36, no. 3, pp. 32–39, May 2022.

[200] Y. He, K. Huang, G. Zhang, F. R. Yu, J. Chen, and J. Li, “Bift: A blockchain-based federated learning system for connected and autonomous vehicles,” IEEE Internet Things J., vol. 9, no. 14, pp. 12311–12322, Jul. 2022.
[201] H. Liu et al., “Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing,” IEEE Trans. Veh. Technol., vol. 70, no. 6, pp. 6073–6084, Jun. 2021.
[202] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam, and O. M. Elkomy, “Federated intrusion detection in blockchain-based smart transportation systems,” IEEE Trans. Intell. Transp. Syst., vol. 23, no. 3, pp. 2523–2537, Mar. 2022.
[203] A. A. Khan, M. M. Khan, K. M. Khan, J. Arshad, and F. Ahmad, “A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs,” Comput. Netw., vol. 196, Sep. 2021, Art. no. 108217.
[204] D. Jadav, M. S. Obaidiat, S. Tanwar, R. Gupta, and K.-F. Hsiao, “Amalgamation of blockchain and AI to classify malicious behavior of autonomous vehicles,” in Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS), Nov. 2021, pp. 1–5.
[205] D. Patel et al., “Deep learning and blockchain-based framework to detect malware in autonomous vehicles,” in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), May 2022, pp. 278–283.
[206] H. Moniz, “The Istanbul BFT consensus algorithm,” 2020, arXiv:2002.03613.
[207] J. Khamar and H. Patel, “An extensive survey on consensus mechanisms for blockchain technology,” in Data Science and Intelligent Applications. Cham, Switzerland: Springer, 2021, pp. 363–374.
[208] Y. Fu, F. R. Yu, C. Li, T. H. Luan, and Y. Zhang, “Vehicular blockchainbased collective learning for connected and autonomous vehicles,” IEEE Wireless Commun., vol. 27, no. 2, pp. 197–203, Apr. 2020.
[209] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, “Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles,” IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4298–4311, Apr. 2020.
[210] I. Aliyu, M. C. Feliciano, S. van Engelenburg, D. O. Kim, and C. G. Lim, “A blockchain-based federated forest for SDN-enabled invehicle network intrusion detection system,” IEEE Access, vol. 9, pp. 102593–102608, 2021.
[211] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” Internet Things, vol. 11, Sep. 2020, Art. no. 100227.
[212] K. Salah, M. Rehman, N. Nizamuddin, and A. Al-Fuqaha, “Blockchain for AI: Review and open research challenges,” IEEE Access, vol. 7, pp. 10127–10149, 2019.
[213] K. Khacef, S. Benbernou, M. Ouziri, and M. Younas, “Trade-off between security and scalability in blockchain design: A dynamic sharding approach,” in Proc. Int. Conf. Deep Learn., Big Data Blockchain. Cham, Switzerland: Springer, 2021, pp. 77–90.
[214] M. H. Nasir, J. Arshad, M. M. Khan, M. Fatima, K. Salah, and R. Jayaraman, “Scalable blockchains—A systematic review,” Future Gener. Comput. Syst., vol. 126, pp. 136–162, Jan. 2022.

[215] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras, and I. Stamelos, “Securing emission data of smart vehicles with blockchain and selfsovereign identities,” in Proc. IEEE Int. Conf. Blockchain (Blockchain), Nov. 2020, pp. 462–469.
[216] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, and C. Zhang, “Towards secure network computing services for lightweight clients using blockchain,” Wireless Commun. Mobile Comput., vol. 2018, pp. 1–12, Nov. 2018.
[217] R. Gupta, A. Kumari, and S. Tanwar, “A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles,” Trans. Emerg. Telecommun. Technol., vol. 32, no. 6, Jun. 2021, Art. no. e4009.
[218] L. Creutz, J. Schneider, and G. Dartmann, “Fides: Distributed cyberphysical contracts,” in Proc. 3rd IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA), Dec. 2021, pp. 51–60.
[219] S. Lockey et al., “A review of trust in artificial intelligence: Challenges, vulnerabilities and future directions,” in Proc. Annu. Hawaii Int. Conf. Syst. Sci. Hawaii Int. Conf. Syst. Sci., 2021, 5463–5472.
[220] A. R. Singh, H. Singh, and A. Anand, “Vulnerability assessment, risk, and challenges associated with automated vehicles based on artificial intelligence,” in Advances in Communication and Computational Technology. Cham, Switzerland: Springer, 2021, pp. 1323–1337.
[221] T. Evas. European Framework on Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies. Accessed: Jan. 14, 2022. [Online]. Available: shorturl.at/filqK
[222] M. Scalas and G. Giacinto, “On the role of explainable machine learning for secure smart vehicles,” in Proc. AEIT Int. Conf. Electr. Electron. Technol. Automot. (AEIT AUTOMOTIVE), Nov. 2020, pp. 1–6.
[223] M. H. Kabir, K. F. Hasan, M. K. Hasan, and K. Ansari, “Explainable artificial intelligence for smart city application: A secure and trusted platform,” 2021, arXiv:2111.00601.
[224] M. Mongelli, “Design of countermeasure to packet falsification in vehicle platooning by explainable artificial intelligence,” Comput. Commun., vol. 179, pp. 166–174, Nov. 2021.
[225] F. Costantini, N. Thomopoulos, F. Steibel, A. Curl, G. Lugano, and T. Kováˇciková, “Autonomous vehicles in a GDPR era: An international comparison,” in Advances in Transport Policy and Planning, vol. 5. Amsterdam, The Netherlands: Elsevier, 2020, pp. 191–213.
[226] V. Ilkova and A. Ilka, “Legal aspects of autonomous vehicles—An overview,” in Proc. 21st Int. Conf. Process Control (PC), Jun. 2017, pp. 428–433.
[227] A European Approach to Artificial Intelligence. Accessed: Jan. 28, 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[228] Blockchain Strategy. Accessed: Jan. 28, 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy
[229] A. B. Arrieta et al., “Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI,” Inf. Fusion, vol. 58, pp. 82–115, Jun. 2020.
[230] I. Bashir, “Quantum consensus,” in Blockchain Consensus. Cham, Switzerland: Springer, 2022, pp. 377–409.

[231] D. B. Abdullah and H. H. Mohammed, “Computation offloading in the internet of connected vehicles: A systematic literature survey,” J. Phys., Conf. Ser., vol. 1818, no. 1, Mar. 2021, Art. no. 012122.
[232] M. Aazam, S. Zeadally, and K. A. Harras, “Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities,” Future Gener. Comput. Syst., vol. 87, pp. 278–289, Oct. 2018.

Fig. 1. Levels of driving automation.

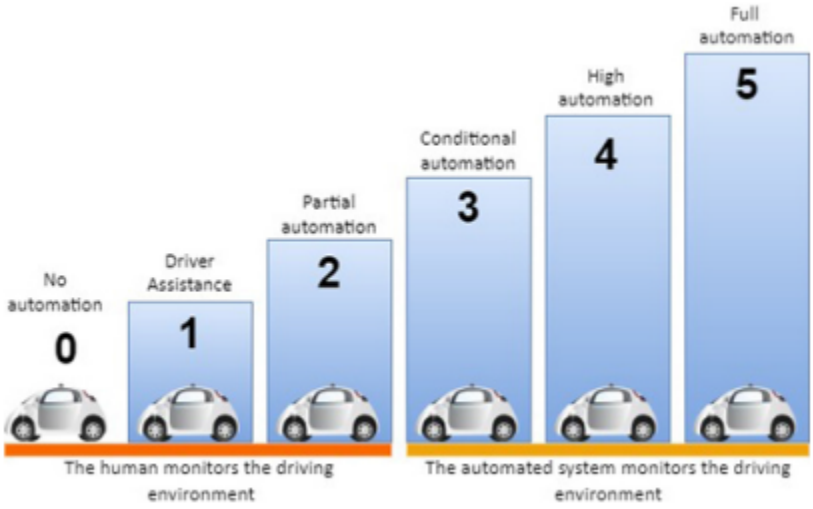

Fig. 2. AV sensing components [20].

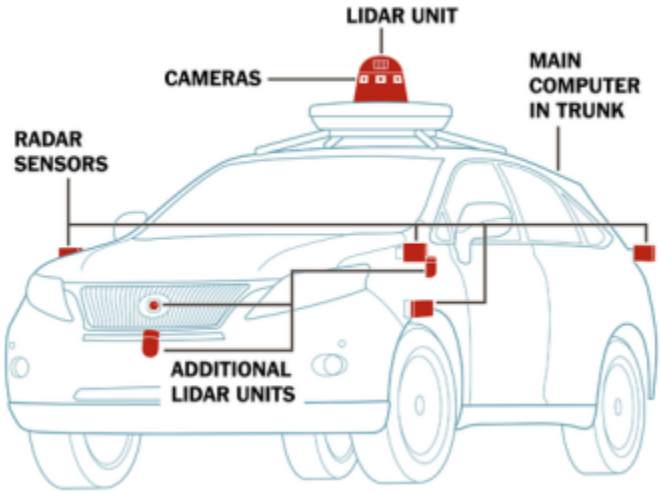

Fig. 3. V2X communication for autonomous vehicles.

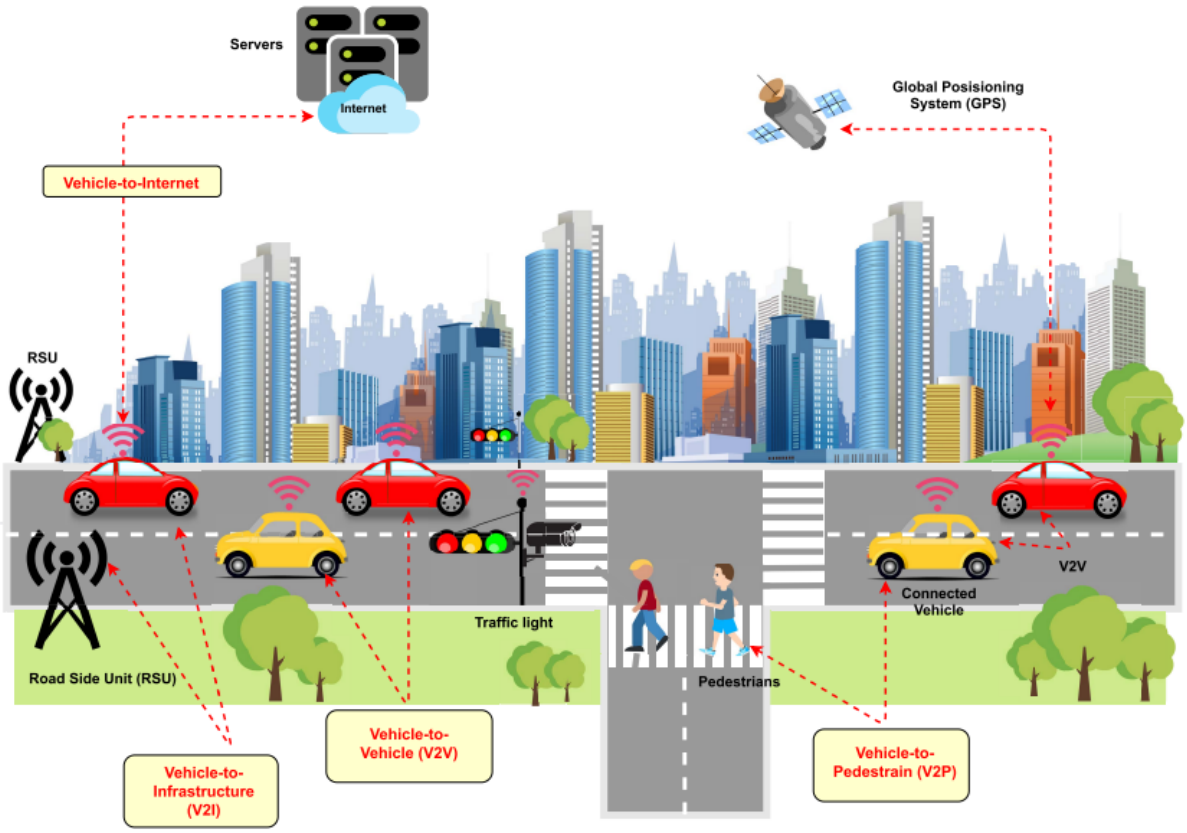

Fig. 4. Most hackable points of AV and AV communication networks

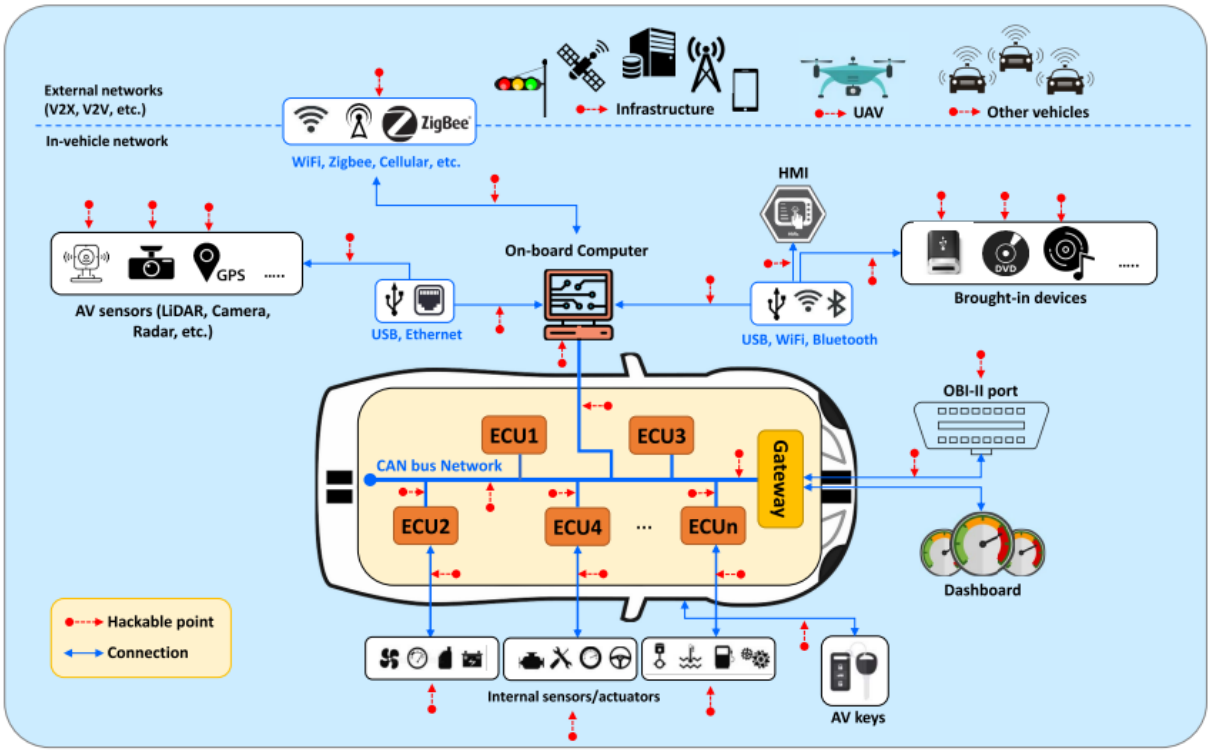

Fig. 5. Classification of major security and privacy threats for AVs.

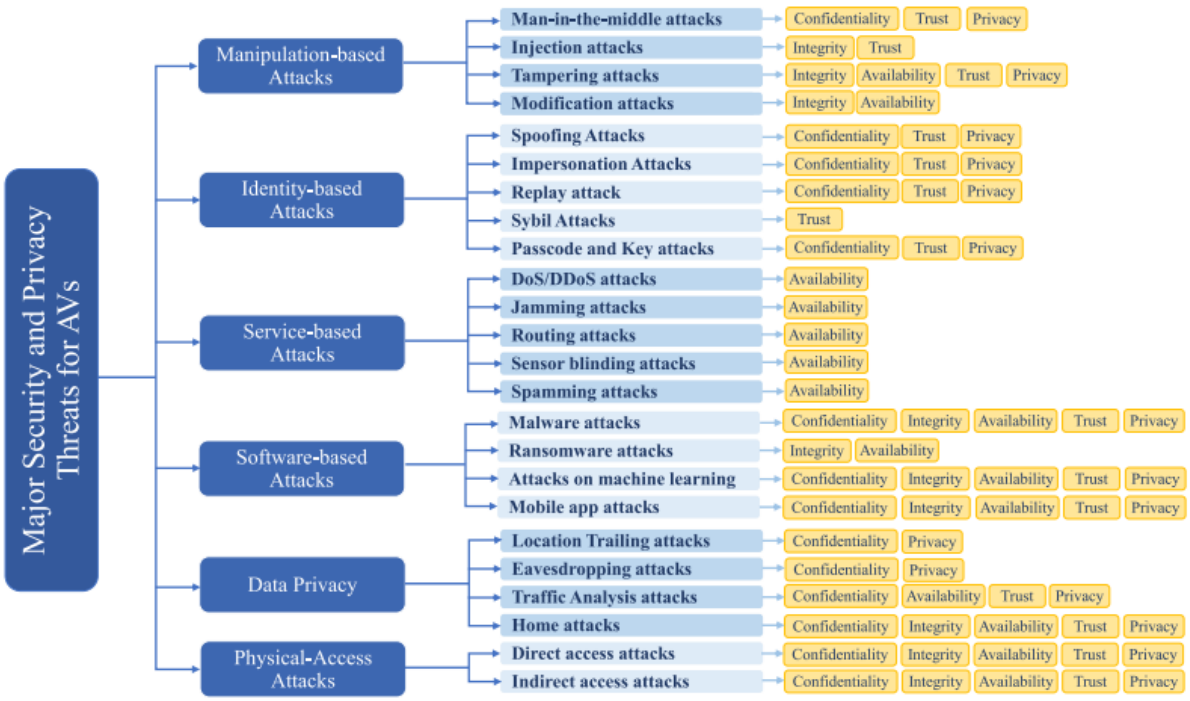

Fig. 6. Comparison of the learning techniques.

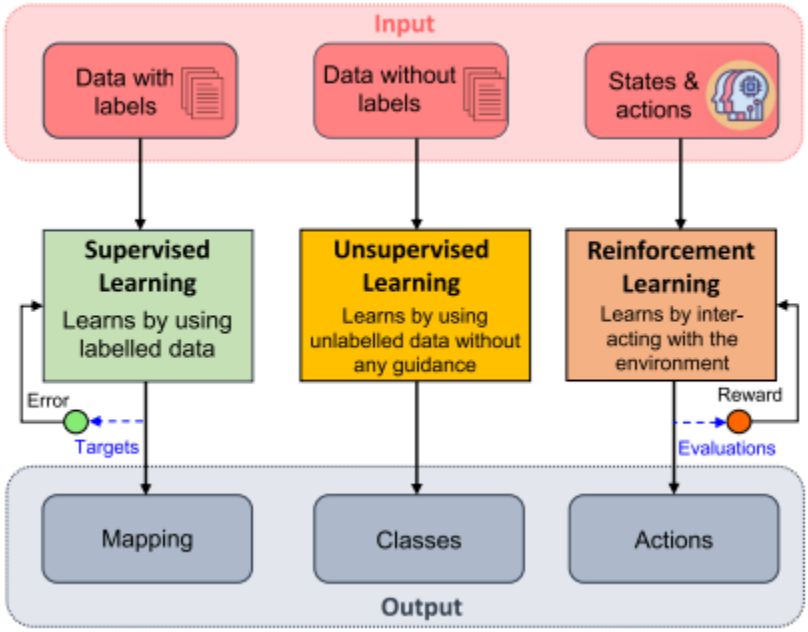

TABLE I
MAIN FEATURES OF PUBLIC, PRIVATE, AND CONSORTIUM BC [13]

Features	Public BC	Private BC	consortium BC
Access	All	Single company	Several companies
Identity	Anonymous	Approved	Approved
Immutability	Yes	Partial	Partial
Speed	Slow	Fast	Fast
Cost	High	Low	Low
Privacy	No privacy	High privacy	High privacy
Centralised	No	Partial	Partial
Scalability	Low	Medium	Medium

TABLE II
EXAMPLES OF RECENT BC-BASED SOLUTIONS RELATED TO AVS SECURITY AND PRIVACY

Application scenarios	Authors	Year	Description	Blockchain Platform
Secure Data Storage	Jiang et al. [96]	2019	Secure storage of the AV data in the cloud	Ethereum
	Zhang et al. [97]	2019	Secure data storage and sharing between AVs and RSUs	Consortium BC
	Singh et al. [98]	2021	Storage of five categories of AV data in five BC	Public/Private BCs
	Yin et al. [96]	2021	Data storage system with incremental AV data updating	Ethereum
	Riya et al. [99]	2022	Secure data storage and sharing among AVs	Ethereum
	Meghna et al. [100]	2022	Encrypting and hashing the AV data for secure storage	Private BC
Secure Communication Channels	Singh et al. [101]	2017	Securing V2V communications & privacy protection	Private BC
	Rowan et al. [102]	2017	Securing V2V communications (V2V network)	Ethereum
	Yang et al. [103]	2018	Securing the communications between AVs and RSUs	Bitcoin
	Mitra et al. [22]	2018	BC-based V2V data aggregation model	Hyperledger Fabric
	Rathee et al. [104]	2019	Securing Smart sensors of AVs (In-Vehicle Network)	Ethereum
	Oham et al. [105]	2021	Securing the in-vehicle network components	Private BC
	Dakshita et al. [83]	2021	Secure sensing and tracking of AVs	Ethereum
	Wang et al. [106]	2021	Secure routing for swarm UAS networking	Lightweight BC
	Kamal et al. [107]	2021	BC-based system for secure V2V Communication	Public BC
	Ali et al. [108]	2022	BC-based secure V2V communication using ICN network	Public BC
Data Integrity and privacy	Cebe et al. [109]	2018	Records all necessary data for an AV forensics solution	Permissioned BC
	Li et al. [110]	2018	Protecting the AV identity and location privacy	IoTChain [111]
	Davi et al. [112]	2019	Ensure safety and information integrity inside the AV	Bitcoin
	Narbayeva et al. [113]	2020	Data integrity by tracking the actions of AVs	Exonum platform
	Rathore et al. [114]	2020	Protection against data tempering attacks in AV network	IOTA Tangle DLT
	Jha et al. [115]	2022	BC-key management framework and hashgraphs	Permissioned BC
Forensics applications	Cebe et al. [109]	2018	Fragmented ledger for forensic analysis of traffic accidents	Lightweight BC
	Li et al. [116]	2021	Event recording system for vehicular digital forensics	Ethereum
	Yao et al. [117]	2022	BC-based accident responsibility identification model	Lightweight BC
	Oham et al. [105]	2022	BC-based reputation system for AVs accident forensics	Permissioned BC
Reputation & Trust Management	Kang et al. [118]	2019	Data sharing in V2V using reputation and contract theory	Public BC
	Abbes et al. [119]	2021	BC-based solution for reputation management in IoV	Ethereum
	Lee et al. [120]	2021	Two-layered AV reputation BC system	Private/Public BCs
	Bhattacharya et al. [121]	2022	BC-based trust scheme for cellular V2X ecosystems	Consortium BC
	Kianersi et al. [122]	2022	BC-based reputation system for secure V2V communications	Public BC

TABLE III
EXAMPLES OF RECENT AI-BASED SOLUTIONS RELATED TO AVS SECURITY AND PRIVACY

Application scenarios	Authors	Year	Description	AI model used
ML/DL-based Intrusion Detection, Prevention Systems (IDSs, IPSs)	Berger et al. [152]	2018	Anomaly detection within automotive CAN networks of AVs	SVM, OCSVM, NN
	Lokman et al. [153]	2019	Anomaly detection in the in-vehicle network	DCAEs
	Yang et al. [154]	2020	Identification of spoofing attacks in CAN bus	LSTM, RNN
	Theyazn et al. [151]	2022	Detection of flooding, fuzzing, spoofing and replaying attacks in CAN	LSTM, CNN
	Otoum et al. [155]	2021	Anomaly detection in intra-vehicles and external networks	DBN, RF
	Mehedi et al. [156]	2021	Detection of flooding, fuzzing and spoofing in the In-Vehicle Network	DTL
	Ahmed et al. [157]	2020	Mitigation of relay attacks on PKE and Start (PKES) systems of AV	DT, K-NN, CVM
	Kavousi et al. [158]	2020	Classification of the messages between ECU and other hardware in AV	GAN
	Haider et al. [159]	2018	Proactive anomaly detection to a use-case of hijacked connected AVs	RBE
	Kashyap et al. [160]	2021	Identification of malicious vehicles behaviour	GP
	Khan et al. [161]	2022	Classification of adversarial attacks	TDL
	Aldhyani et al. [151]	2022	Detect message attacks against in-vehicle CAN buses	CNN, LSTM
	Zhang et al. [162]	2022	Intrusion Detection for In-Vehicle Networks	DNN
Malware Analysis and Classification	Han et al. [60]	2021	Identification and classification of malware in self-driving systems	k-NN
	Catal et al. [163]	2021	Malware detection models using Graph Attention Networks (GAN)	GAN
	Rahal et al. [164]	2022	Bot malware detection in vehicular networks	NB, SVM, K-NN
Reputation & Trust Management	Zhang et al. [148]	2018	Trust management in vehicular ad hoc networks (VANETs) of AVs	DRL
	Gyawali et al. [147]	2021	Limitation of the wrong feedbacks from malicious vehicles	Q-learning, DNN
	Eziama et al . [165]	2018	Classification of of honest and dishonest vehicles in the network	BNN
	Karmakar et al. [166]	2021	Measure the trustworthiness of AV and its major OBU components	DNN
	Mankodiya et al. [167]	2021	XAI for trust management in AVs	XAI, RF, DT
	Zhang et al. [168]	2022	SDN-based trust model for securing AV communication	Q-learning, DNN
Data Privacy and Integrity	Li et al [169]	2021	Preserve AV privacy by keeping original data in a local vehicle	FL
	Lu et al. [170]	2020	Enhance data privacy and mitigation of data leakage in AV systems	FL, CNN
	Aashma et al. [171]	2021	Privacy preserving and misbehavior detection in AVs networks	FL, ANN
	Min et al. [172]	2021	AV Location data privacy protection in vehicular networks	RL

TABLE IV
DIFFERENT ASPECTS BETWEEN AI AND BLOCKCHAIN [184]

Aspects	AI	BC
Nature	Centralized	Decentralized
Access	Closed	Open
Transparency	Black Box	Transparent
Approach	Probabilistic	Deterministic

TABLE V
DEFENSE RESEARCH RELATED AVS SECURITY AND PRIVACY USING BOTH BC AND AI TECHNIQUES

Application scenario	Authors	Year	Description	BC used	AI model[1]
Secure Communication Channels	Xia et al. [145]	2021	Secure information sharing in V2X network	Consortium BC	LSTM
	Rabieinejad et al. [193]	2021	Secure V2X communication	Public BC	DNN
	CUB project [12]	2022	Protect the in-vehicle and V2X networks	Private/Public BC	DL, RL
	Raja et al. [194]	2022	Secure Cooperative Adaptive Cruise Control (CACC)	Permissioned BC	Deep RL
Data Privacy and Integrity	Qian et al. [195]	2020	Preserve data privacy between AVs and RSUs	Public BC	ML, DL
	Pokhrel et al. [181]	2020	Privacy-aware and secure V2X communications	Public BC	FL, ML
	Hammoud et al. [190]	2020	Protection against undesirable data modification in AVs	Hybrid BC	RL
	K. Lo et al. [196]	2022	Privacy of knowledge during the learning process	Consortium BC	FL, ML
Collaborative Learning	Pokhrel et al. [191]	2020	Secure collective learning in V2X network	vDLT BC	TF
	Chai et al. [197]	2020	Preserve learning data privacy in X2V communication	Public BC	FL, ML
	Dajun et al. [198]	2022	Secure cooperative learning framework for AVs	Permissioned BC	DL
	Barbieri et al. [192]	2022	Secure collaborative learning in 6G V2X networks	Public BC	FL
	Kumar et al. [199]	2022	Collaborative learning for secure V2X communications	Public BC	FL, SL
	He et al. [200]	2022	Privacy-preserving ML process for connected AVs	Consortium BC	FL
Collaborative Intrusion Detection	Lui et al. [201]	2021	Collaborative Intrusion Detection in V2X network	Ethereum BC	DNN, FL
	Mohamed et al [202]	2021	Collaborative intrusion detection framework for AVs	Hybrid BC	FL, DL
	Khan et al. [203]	2021	Collaborative intrusion detection within UAVs	Ethereum BC	FL, ML
	Jadav et al. [204]	2021	Collaborative IDS to classify malicious behavior of AVs	Public BC	ML
	Patel et al. [205]	2022	FL and BC-based model to detect Malware in AVs	Ethereum BC	ResNet50

[1] (TF) TensorFlow; (SL) Split Learning