Received: 25 April 2023 | Revised: 10 August 2023 | Accepted: 12 August 2023

DOI: 10.1002/widm.1515

ADVANCED REVIEW

WIREs DATA MINING AND KNOWLEDGE DISCOVERY

WILEY

Machine learning and blockchain technologies for cybersecurity in connected vehicles

Jameel Ahmad[1] | **Muhammad Umer Zia**[2] | **Ijaz Haider Naqvi**[3] | **Jawwad Nasar Chattha**[4] | **Faran Awais Butt**[4] | **Tao Huang**[2] | **Wei Xiang**[5]

[1]Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan

[2]College of Science and Engineering, James Cook University, Cairns, Australia

[3]School of Science and Engineering, Lahore University of Management Sciences, DHA, Lahore, Pakistan

[4]Department of Electrical Engineering, School of Engineering, University of Management and Technology, Lahore, Pakistan

[5]School of Computing, Engineering and Mathematical Sciences, La Trobe University, Melbourne, Victoria, Australia

Correspondence
Wei Xiang, School of Computing, Engineering Mathematical Sciences, La Trobe University, Melbourne, VIC, Australia.
Email: w.xiang@latrobe.edu.au

Edited by: Tianrui Li, Associate Editor and Witold Pedrycz, Editor-in-Chief

Abstract

Future connected and autonomous vehicles (CAVs) must be secured against cyberattacks for their everyday functions on the road so that safety of passengers and vehicles can be ensured. This article presents a holistic review of cybersecurity attacks on sensors and threats regarding multi-modal sensor fusion. A comprehensive review of cyberattacks on intra-vehicle and inter-vehicle communications is presented afterward. Besides the analysis of conventional cybersecurity threats and countermeasures for CAV systems, a detailed review of modern machine learning, federated learning, and blockchain approach is also conducted to safeguard CAVs. Machine learning and data mining-aided intrusion detection systems and other countermeasures dealing with these challenges are elaborated at the end of the related section. In the last section, research challenges and future directions are identified.

This article is categorized under:

Commercial, Legal, and Ethical Issues > Security and Privacy

Technologies > Machine Learning

Technologies > Internet of Things

KEYWORDS

blockchain, connected and autonomous vehicles, cybersecurity, deep learning, federated learning, internet of vehicles

1 | INTRODUCTION

Cybersecurity refers to technologies, tested processes, and professional practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity may also be referred to as information technology security. Securing a system's information flow is a gigantic issue because of the numerous types of possible attacks/threats, that is why cybersecurity experts are emphasizing a customized security system for modern-era domains such as healthcare (Naresh & Thamarai, 2023), Telemetry (Abreu & Pereira, 2022), IoT (Almagrabi, 2023), and other systems with big data analytics (Pramanik et al., 2021). The general communication framework for emerging connected and autonomous vehicles poses a severe security challenge as its safety can be compromised by several diverse

types of cyberattacks. Moreover, there are still a lot of uncertainties and doubts about cause-effect relationships and mechanisms of vehicles' cybersecurity. We will provide a holistic perspective on different cybersecurity threats, detection mechanisms, and possible mitigation techniques.

To understand various security vulnerabilities, we need to discuss the communication techniques deployed in connected and autonomous vehicles (CAVs) which can be divided into two basic categories. The first is intra-vehicle, and the second is inter-vehicle communication (Möller et al., 2018). Intra-vehicle communications enable the automation of autonomous vehicles with aid of data/information collected from onboard sensors. In this mode, CAVs do not communicate or cooperate with other CAVs and smart infrastructure. On the other hand, inter-vehicle communications are based on a cooperative model to enable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Depending on these two basic types of communications, there are different attack surfaces through which a hacker can attack smart vehicles. The vulnerabilities associated with inter and intra-vehicular communications can either be exploited from close proximity or remotely and can affect communication as well as multi-modal sensors such as ultrasonic, infrared, and vision sensors.

The onboard diagnostics (OBD) system of a CAV tracks the vehicle's performance and allows the CAV to communicate any problem inside the vehicle and data collected by the sensors to the outside world (Ivanov et al., 2018). A hacker can attack the vehicle remotely through one of the OBD ports. Onboard units in CAVs use dedicated short-range communication (DSRC; Xiong et al., 2017) with different standards introduced by the Institute of Electrical and Electronics Engineers (IEEE) such as IEEE 1609.3 (Eiza & Ni, 2017). These DSRC onboard units thus create opportunities for hackers to attack smart vehicles by sending false signals via these units.

Remote vulnerability can also be exploited through malware attacks. Malware attacks are those cyber threats that enable hackers to cause damage by introducing malicious software into a computing system (Batres et al., 2016). Several malware types can hinder or halt the normal operations of a network, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper, scareware, and so forth. The electronic control unit, its software as well as software updates that give computing power to autonomous vehicles, also make CAVs vulnerable to aforementioned malware attacks. Some CAVs also have the option to connect them to mobile applications; for example, Apple has car play, and Google has android auto interfaces. These mobile applications involve many risks and make autonomous vehicles vulnerable to cyberattacks. By sending a malicious/malware code through these applications, a hacker can obtain personal data and cause damage to the vehicle, as occurred in the Nissan connect application vulnerability case (Eiza & Ni, 2017). The dimensions of CAVs' security requirements, threats, and countermeasures discussed in this article are presented in Figure 1.

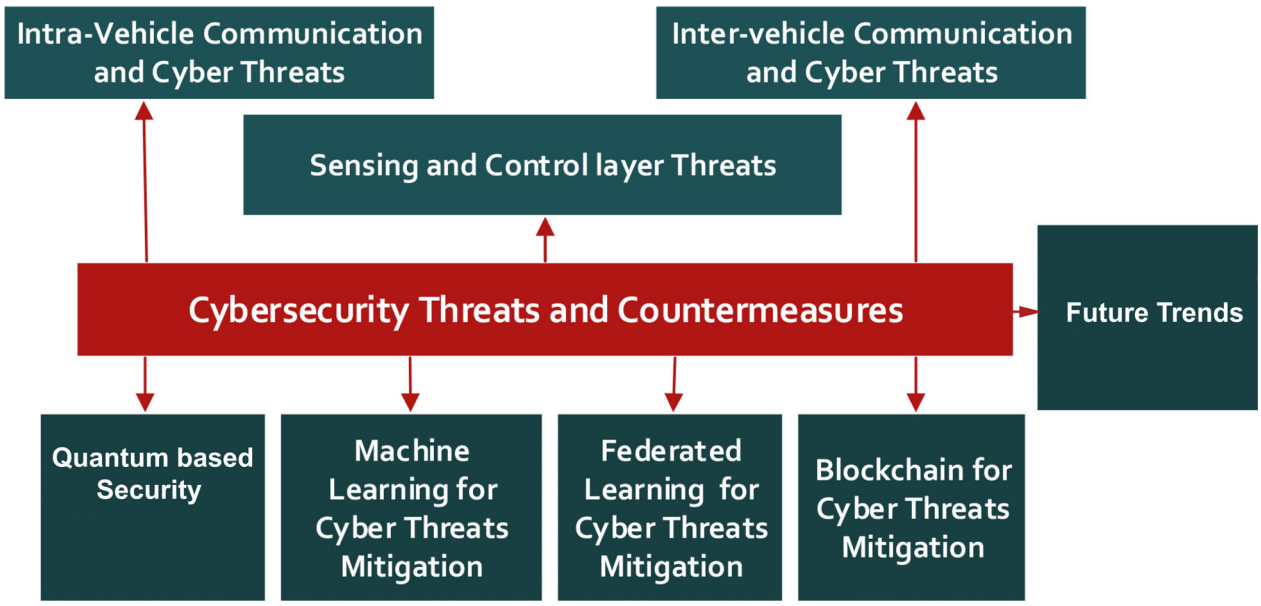

FIGURE 1 Cybersecurity threats and countermeasures for CAVs.

1.1 | Requirements of secure vehicles

The CAV network poses severe security challenges and tackling these challenges has become a potential research impetus for the automotive industry. The internet connectivity modes, as well as V2V and V2I communications, make CAVs vulnerable to potential malicious cyberattacks. A CAV contains many electronic control units that can be exploited during a cyberattack. Moreover, most of CAVs are equipped with a large number of sensors for environment sensing, thus creating an opportunity for cyberattacks on sensors, and the functionality of these vehicles can be compromised (Aijaz et al., 2006; Axelrod, 2017; Axelrod, 2018; Cui et al., 2018; Ning et al., 2013; Parkinson et al., 2017; Straub et al., 2017; Trotter et al., 2018). The data acquisition sensors like Light Detection and Ranging (LiDAR), Radio Detection and Ranging (RADAR), Global Positioning System (GPS), Inertial Measurement Unit (IMU), cameras, and ultrasonic sensors send information to a high-speed onboard computer for real-time signal processing and subsequent scene perception or other decision-making tasks. Hackers' access to this sensory data violates the privacy of a CAV and in extreme cases handovers total control of the vehicle to the adversary. In 2016, the National Highway Traffic Safety Administration (NHTSA), a federal government agency of the United States, issued a report and warned CAV users about potential cyberattacks (Eiza & Ni, 2017). Some of the attacks mentioned in the report resulted in sudden engine shutdowns, brake failure, and locked windows/doors. Hackers can hack into the vulnerable connected vehicles either within the communication range or from miles away through the Internet. The design of secure and successful intelligent vehicular cyberphysical systems depends on developing a fool-proof security framework (Bhat et al., 2018; Chattopadhyay et al., 2020; El-Rewini, Sadatsharan, Selvaraj, et al., 2020; El-Rewini, Sadatsharan, Sugunaraj, et al., 2020; Kelarestaghi et al., 2019). To combat all types of threats, all forms of communication must meet the common security requirements accepted worldwide as a key to a secure communications system (Chowdhury et al., 2020). These four requirements are Authentication, Integrity, Privacy, and Availability. Identifying appropriate security requirements and developing a security system accordingly plays a key role in securing CAVs and its occupants.

Vehicle manufacturers are working hard to improve the ability of vehicles to detect and respond to threats. Over time, they have become more aware that hackers can deceive them and the fact that leak of vehicle sensory data can cause havoc on the road (Garakani et al., 2018). Moreover, vehicle manufacturers are aware that attackers can exploit connected and automated vehicles by hacking roadside infrastructure and stealing ride-hailing user data stored in the cloud. Over-the-air updates enable automakers to apply software updates and fix bugs remotely. However, this can lead to security issues because a simple faulty patch can cause system malfunctioning and confusion (Wan et al., 2019). These updates are sent and initiated remotely, so the risk of exploitation is high if the security posture of such updates is not well implemented.

1.2 | Research scope and contributions

Section-wise breakdown of the article is given in Figure 2. This survey aims to provide a comprehensive view of state-of-the-art technology, practices, and future trends concerning CAVs' security. Hereby, the key contributions of our research are as follows:

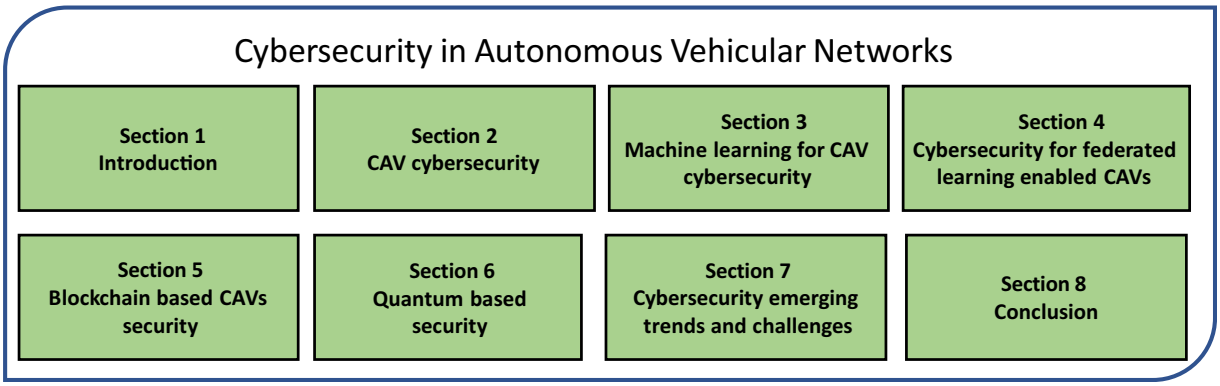

FIGURE 2 Section breakdown.

1. A comprehensive system-level overview is conducted concerning the cyberattacks arising from diverse dimensions such as inter and intra-vehicular communication, machine learning, and quantum computing-based attacks. After each section, the possible countermeasures concerning the attack dimension are elaborated.
2. Along with the understanding of the cyberattacks of various types in CAVs, this investigation analyses if the countermeasures are sufficient to safeguard future CAVs, or do we need more counter-countermeasures to prevent cyberattacks.
3. A detailed overview of the latest machine learning, federated learning, and blockchain technologies and their impact on CAV's security is presented. We also conducted a detailed discussion of security measures in order to minimize the potential risks and maximize the security benefits of the latest technologies.
4. This article explores data mining techniques for enhancing intrusion detection systems and their capabilities in connected and autonomous vehicles.

Current literature only partially answers these questions. The aspects covered in current literature alongside our survey are presented in Table 1. This article goes beyond these previous efforts and focuses on crossovers between communications, control, artificial intelligence, federated learning, blockchain, and cybersecurity. Unlike surveys and tutorials covering a limited set of topics related to CAVs, we review a system of systems integrated approach in intelligent vehicles. We also review applications not looked at in other related surveys, including communications analytics affecting traffic flow, blockchain integration and use case scenarios, security, and privacy in CAVs from a machine and federated learning perspective.

While keeping the main scope on cybersecurity of CAVs in the V2V and V2X domains, our article distinguishes itself from earlier surveys in the following perspective: We provide a walk-through of conventional cybersecurity methods applied to CAVs and a holistic perspective on cyberattacks targeting state-of-the-art deep and federated learning approaches, their countermeasures, as well as blockchain-enabled CAVs designs.

2 | CAV CYBERSECURITY

This section will provide a holistic perspective on communications in connected vehicles, different cybersecurity threats, threat bodies, detection mechanisms, and possible mitigation techniques. In intra-vehicle communications, the automation of autonomous vehicles depends entirely on data/information collected from onboard sensors of the autonomous vehicle, and CAVs do not communicate or cooperate with other CAVs/smart infrastructure. On the other hand, inter-vehicle communications are based on a cooperative CAV model to enable V2V and V2I communications. Depending on these two basic types of communications, there are different attack surfaces through which a hacker can attack a vehicle.

TABLE 1 Literature comparison.

Detail research analysis	Conventional attacks	Conventional attacks countermeasures	DL/ML attacks	DL attacks countermeasures	FL threats mitigation	Blockchain enabled designs	Trends and future directions
(El-Rewini, Sadatsharan, Selvaraj, et al., 2020)	✓	✓	×	×	×	✓	×
(Chowdhury et al., 2020)	✓	✓	×	×	×	×	✓
(Dibaei et al., 2020)	✓	✓	×	×	×	×	✓
(Sun, Yu, & Zhang, 2021)	✓	✓	×	×	×	×	✓
(Kim et al., 2021)	✓	✓	×	×	×	×	✓
Ours	✓	✓	✓	✓	✓	✓	✓

In connected and autonomous vehicles, three types of vulnerabilities are possible, namely, physical access vulnerability, close proximity vulnerability, and remote access vulnerability (Petit & Shladover, 2014; Wyglinski et al., 2013). In physical access vulnerability, there are various vulnerabilities that an adversary can exploit, that is, remove, replace legitimate hardware or deploy malicious hardware parts such as altered electronic control units (ECUs), or attack the CAN bus and reprogram the ECUs. Some important electronic control units in autonomous vehicles include the engine control module (ECM), the electronic brake control module (EBCM), the vehicle vision system (VVS), the navigation control module (NCM), the remote door lock receiver, the heating ventilation and air conditioning (HVAC) unit, and, the transmission control module (TCM), and so forth. In close-proximity vulnerability, hackers can interfere or inject malicious data and tamper with onboard sensors like ultrasonic or infrared sensors. Moreover, a malicious activity that creates interference with LiDAR sensors or attacks on vision systems such as cameras of an autonomous vehicle is a serious close proximity vulnerability. Similarly, hackers can also attack different sensors and send wrong signals to these sensors to stop or jam certain functionality of a vehicle (Wyglinski et al., 2013).

DSRC units send and receive data to and from other DSRC units in V2V and V2I settings. These DSRC onboard units thus create another opportunity for hackers to attack the vehicle (either from close proximity or remotely) by sending false signals through these units. The CAVs connection to mobile applications also open doors to several remote cyberattacks vulnerabilities. There are a lot of malicious activities that a hacker can perform by launching malware attacks using remote access vulnerability. For example, it can turn the radio on and off in the vehicle, open or close the door, jam the anti-lock braking system, and send false signals from one vehicle to the other.

Researchers have conducted several investigations to identify and classify the cybersecurity of a CAV system. For example, in the investigation by Tolba and Altameem (2019), a three-tier hierarchical system is used to classify automotive security threats. The sensing layer, also known as the AutoVSCC (Autonomous Vehicular Sensing Communication and Control) framework, is the first layer of the hierarchy and is made up of vehicular sensors. The sensing layer's threats include jamming GPS, eavesdropping on communications of sensor data, and deceiving ultrasonic sensors, and so forth. Threats to the sensing layer can be transmitted to the communication layer via the physical data link interface, which converts analog data from sensors into digital information. In the communication layer, cybersecurity threats include sending incorrect messages, gaining control of vehicle functions via infotainment and telematics systems, and eavesdropping on messages sent between vehicles. The sensing and communication layer's threats can impair the control layer's ability to transport and translate valuable digital data into real-time vehicular applications such as automated steering control, lane change maneuvers, and brake application. Severity of attacks differs based on the scenario and damage that can be done by the attacker. For example, among the potential attack surfaces of autonomous vehicles, GPS spoofing and camera blindness come under the category of high threats, whereas, RADAR confusion, LiDAR confusion, and exploitation of in-vehicle devices and sensors come under the category of medium threats (Petit & Shladover, 2014).

2.1 | Cyberattacks on sensors and countermeasures

CAV sensors can be classified into two major categories, that is, environment and dynamic (El-Rewini, Sadatsharan, Selvaraj, et al., 2020; El-Rewini, Sadatsharan, Sugunaraj, et al., 2020). Many works have been reviewed for different attacks on environmental sensors such as the GPS, millimeter-wave RADAR, LiDAR, ultrasonic sensors, and cameras (Ren, Wang, 2020; Ren, Zheng, et al., 2020). These sensors measure the parameters exterior of the vehicle and provide data to advance driver assistance systems. Spoofing and jamming are two major attacks on the GPS. Spoofing aims to take the vehicle to unauthorized locations by introducing spurious signals. This happens when the victim's car uses Google maps. Spurious signals can be easily detected as the signal looks different from typical satellite signals. Adding location verification, cryptography, cooperative GPS receiver through information exchange with neighboring vehicles, and using message authentication can defend vehicle's GPS from spoofing and jamming attacks (Heng et al., 2015; Milaat & Liu, 2018; Souli et al., 2020). A summary of cyberattacks and countermeasures concerning CAV sensors is presented in Table 2.

RADAR sensors on the vehicle emit electromagnetic signals in the millimeter-wave (mmW) range to measure speed and distance to neighboring vehicles with their penetration capability in smoke, fog, dust, and snow. Long-range RADARs are used for adaptive cruise control and mid-range for assisting in lane change. Due to mmW, such RADARs are of low horizontal resolution and low lateral detection accuracy (Dibaei et al., 2020). However, the accuracy can be enhanced by using them in conjunction with other sensors, such as a camera in a sensor fusion manner for increased target perception. Jamming and spoofing are the major cyberattack categories for RADAR sensors. The attacker can falsify the original radio frequency signal by tactically sending delayed copies of the original radio frequency signal using

TABLE 2 Summary of cyberattacks and countermeasures for sensors in CAVs.

Sensor type	Signal	Security level	Usage	Cyber threats	Countermeasure
Camera	Visible light	High	Traffic signal, obstacle and lane detection, parking	Blinding with confronted Laser, adversarial image, fake vision, blind spot (Petit & Shladover, 2014; Yan et al., 2016)	(Rangesh & Trivedi, 2019; Zhao et al., 2020)
GPS	Microwave	Low	Navigation and anti-theft	Spoofing and jamming (Souli et al., 2020)	(Haider & Khalid, 2016; Korkmaz, 2017; Modas et al., 2020)
RADAR	mmWave	Medium	Inter-vehicle safe distance, Lane change control, adaptive cruise and ADAS	Spoofing, jamming (Yan et al., 2016)	(Guan et al., 2019; Kapoor et al., 2018; Sun, Balakrishnan, et al., 2021)
LiDAR	Infrared laser	High	Collision avoidance, adaptive cruise control, scene perception	Spoofing, jamming, DoS and replay attack (Pham & Xiong, 2020)	(Kim et al., 2021)
IMU	Electrical	Medium to high	Velocity and acceleration measurement, vehicle orientation	Acoustic perturbations in gyro and accelerometer readings, false road gradient data (Vitale et al., 2020)	(Parkinson et al., 2017)

the digital radio frequency memory (DRFM) technique. Sometimes the term of "replay attack" is used for such a scenario. Interference is also a main threat for RADAR sensors causing distance and speed deception. A hash function approach to provide anti-jamming capability is introduced by Guan et al. (2019). The vehicle equipped with RADAR can send an encrypted signal with a hash function to deceive the jammer. The well-known hash functions include MD5, SHA1, SHA256, SHA384, and SHA512 (Sharma & Mittal, 2019). The Hash function modulated signal from CAV has certain randomness, which can be controlled. Kapoor et al. (2018) developed a Spatio Temporal Challenge Response (STCR) method to detect and deceive spoofing attacks against automotive RADAR. This scheme uses multiple-input multiple-output (MIMO) antennas with beam-forming and transmits signals in various randomly selected directions, while probing the environment and receiving the reflected signals, whereas, at the receiving end, suspicious signals are filtered out with a good estimate of the distance between the host and target vehicle. STCR performs better than Physical Challenge-Response Authentication (PyCRA; Shoukry et al., 2015) by reduction in distance error from 35 to 40 m. PyCRA (Shoukry et al., 2015) provides secure active sensing by continually challenging the surrounding environment via random but deliberate physical probes (Guan et al., 2019; Kapoor et al., 2018).

End-to-end security analysis of mmWave RADAR was conducted by Sun, Balakrishnan, et al. (2021), in which authors reported five real-world attack scenarios where spoofing mmWave sensing module or faking the locations of existing obstacles can lead to fatal accidents. In this work, Lincoln MKZ-based CAV testbed, at the University at Buffalo, equipped with the software-defined radio (SDR) mmWave transceiver system from National Instrument (NI) was used for testing and validation.

Regarding LiDAR, two types of technologies are available for environmental sensing. The first is laser scanning LiDAR, mounted on the vehicle, which uses 3D laser scanning of the surrounding environment for scene perception. The second type is the Solid-state LiDAR which maps the environment without any rotation. Spoofing, jamming, replay, relay, and denial-of-service (DoS) attacks can cause LiDAR's data integrity issues. The attacker may receive laser pulses and can send back a delayed version of the transmitted pulses. The attacker may also inject spurious signals, creating false obstacles for autonomous vehicles. Developing countermeasures for LiDAR data integrity will safeguard vehicles against malicious attacks. In the investigation conducted by Changalvala and Malik (2019), the authors

proposed a data hiding technique based on three-dimensional quantization index modulation (QIM) and inject a binary watermark into the LiDAR data in the sensing layer, which is counter-verified at the decision unit by an Advanced Driver Assistance System (ADAS), for tamper detection. This method can help protect vehicles against fake object insertion (FOI) and target object deletion (TOD). The proposed method was validated using a standard benchmark data set, that is, KITTI. Another scheme that can be effectively utilized is to implement random probing of the LiDAR sensor by continually changing the pulse repetition interval, thus making it difficult for attackers to synchronize their laser to the correct transmitted frequency.

2.2 | Intra-vehicle cyber threats and countermeasures

To securely deploy a network for CAVs, the defense mechanism against several cyber threats must be in place (Carsten et al., 2015). Security threats must be dealt with proactively. However, it is difficult to foretell all potential network threats, and our reactive approaches must be fast and effective to prevent any damage. Moreover, ideally, the system should experience no service disruption caused by an attack and its response (Dibaei et al., 2020). Intra-vehicle communications should be designed to send/receive data to the internal bus system reliably. Cybersecurity attack surfaces and vectors for CAVs are shown in Figure 3. In the following, we will enlist and elaborate on some attacks that affect modern autonomous vehicles and enables transmissions between vehicle ECUs and telematics.

2.2.1 | CAN bus attacks

- Masquerading attacks: A masquerading attack compromises the authentication requirement in which an attacker disguises itself as a genuine node. Liu, Zhang, et al. (2017) and Choi, Joo, et al. (2018) identified a couple of CAN vulnerabilities that can lead to masquerading attacks. An adversary can inspect CAN frames as they are not encrypted before transmission. Moreover, message authentication is unsupported in CAN, so the source cannot be authenticated, which can cause illegitimate frame transmission.
- Eavesdropping attacks: An eavesdropping attack violates privacy. In this type of attack, unauthorized individuals gain access to CAV messages. The broadcast transmissions permitted by CAN bus provide a chance for the adversary to infiltrate the in-vehicle network and identify patterns in legitimate CAN frames (Liu, Zhang, et al., 2017). Furthermore, eavesdropping is also possible on the FlexRay protocol, leading to compromised message privacy. The

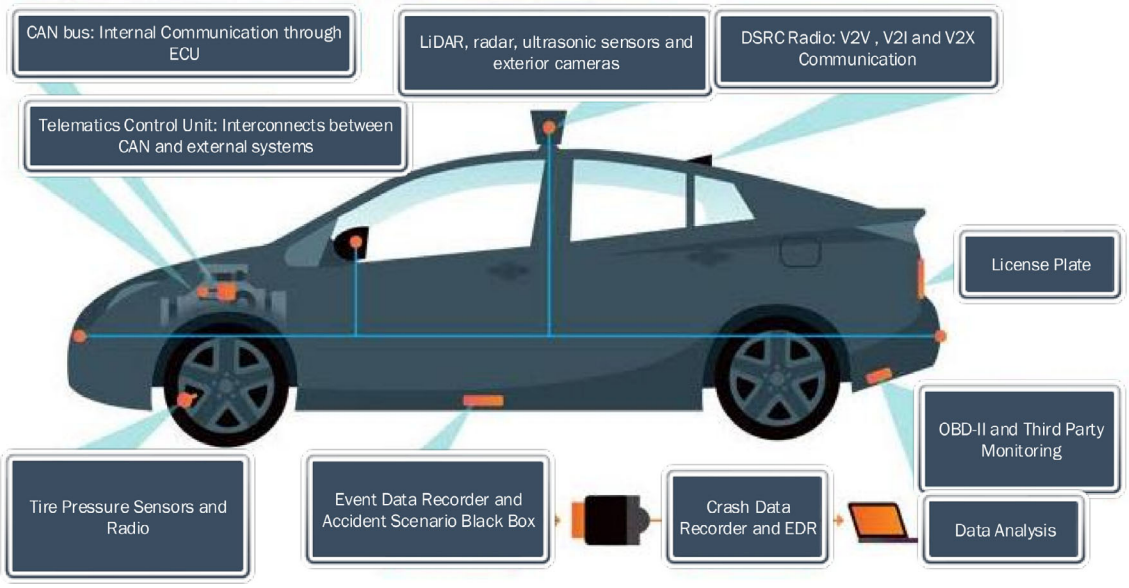

FIGURE 3 Cybersecurity attack vectors in CAVs.

investigation by Mousa et al. (2016) emphasizes that FlexRay and CAN face the same security concerns of possible compromise of security primitives, CAV privacy, and information confidentiality.

- Injection attacks: In this type of attack, a malicious node injects fake messages into an automotive bus system, thus tampering with integrity. The unauthorized access can be acquired to the in-vehicle network by compromised OBD-II ports, ECUs, information and entertainment systems, and telematics systems (Liu, Zhang, et al., 2017). Since conventional CAN systems do not authenticate sending or receiving links, the legitimacy of the frames cannot be validated.
- Replay attacks: The replay attack hinders the integrity and availability of security requirements. In this attack, the adversary consistently and repeatedly sends valid frames to hinder the vehicle's real-time processing or choke transmission (Liu, Zhang, et al., 2017).
- Bus-off attacks: Bus-off attacks abuse integrity by continually sending bits in the identifier field and other fields, which results in the ECU's transmit error counter (TEC) increment. The exceeding value of TEC greater than 255 causes ECU to collapse (Choi, Joo, et al., 2018).
- Denial of service (DoS) attacks: The DoS attack compromises network availability. In DoS, the attacking node continually sends high-priority messages that block genuine low-priority messages (Liu, Zhang, et al., 2017). The identifier segment in a standard CAN packet evaluates the message priority. In this attack, an adversary sets a low value in the identifier segment to assign a high-priority status to the messages. The DoS attacks can be manipulated such that they can lead to control override attacks, which increases their threat potential as an attacker can now take control of the vehicle (Carsten et al., 2015).

2.2.2 | LIN attacks

- Message spoofing attacks: This type of attack defies the authentication requirement by sending illegitimate messages with disinformation to obstruct CAVs communications. A couple of security risks within LIN master–slave communication cause message spoofing attacks (Deng et al., 2017). In a LIN network, message transmission from a master can make slaves sleep. Moreover, the master can use the SYNC field present in the LIN message to synchronize slaves. A node with malicious intentions can exploit the master's abilities to spoof messages and order the slaves to sleep resulting in a complete shutdown of the LIN network. The message spoofing and SYNC field tempering can also cause issues in real-time communication and unexpected network problems.
- Response collision attacks: The response collision attack inhibits data availability by sending an illegal message simultaneous to a legitimate message. The response collision attacks make use of LIN's error handling mechanism, which initiates when a responding slave node acknowledges a conflicting value in the bus and holds transmission. The adversary nodes can victimize this mechanism either by sending a false header or delaying until the master node sends a header, and the adversary can make use of the false message timing, and collision mechanism (Takahashi et al., 2017). This will change the value in the bus leading to a stop transmission stance by legitimate slave nodes. Moreover, the attacker's ability to determine the correct checksum mentioned in responses will make other nodes assume that false messages came from valid sources.
- Header collision attacks: Header collision attacks impede the integrity of the transmission. In these attacks, a malicious node transmits a false header to induce a possible collision with a genuine header (Takahashi et al., 2017). The legitimate header indicates that a slave node is obligated to issue a response, but the attacker's collision specifies a change in the publisher node. In the event of a response by a new publisher node, malicious nodes can execute a response collision attack to insert their false message. Along these lines, an adversary can alter the sequence of responses sent within the LIN bus and take control of the vehicle while traveling.

2.2.3 | FlexRay attacks

- Static segment attacks: A static segment attack is a generic term for an attack that aims at the static segment of the FlexRay communication's authentication and integrity (Gu et al., 2016). The autonomous cybersecurity experts suggest that FlexRay security measures concentrate on the static segment due to its venerability and the dangers it poses if compromised.

2.2.4 | MOST attacks

- Synchronization disruption attacks: In a synchronization disruption attack, a malicious node obstructs MOST integrity by sending false timing frames to distort this synchronization. The MOST masters are the authorized entities that can control synchronization by sending timing frames (Deng et al., 2017).
- Jamming attacks: Jamming attacks cease the availability to send legitimate messages through the MOST protocol. The MOST device's priority assignment enables an attacker to execute a jamming attack by persistently sending fake messages that block genuine lower-priority messages. Jamming attacks are also possible if an attacker continually requests a data channel utilizing the control channel within a MOST transmission (Wolf et al., 2006).

2.2.5 | Ethernet attacks

- Network access attacks: Network access attacks breach authenticity and empower attackers to acquire access to the Ethernet network. These attacks can be conducted in isolation or in support of other categories of attacks. A malicious node can either physically join the Ethernet network utilizing a free switch port (Sommer et al., 2019) or can remotely access the network by user-associated security negligence.
- Traffic confidentiality attacks: This category of attack affects authentication and privacy. Unauthorized access acquired by attackers allows them to tap on network traffic. The knowledge about network topology and structure can be gained either by transmitting messages and analyzing their replies or by attaching listening devices to the host cable/switch for traffic analysis (Sommer et al., 2019). Moreover, a malicious node can take advantage of MAC flooding attacks and eavesdrop on all frames.
- Traffic integrity attacks: As the name implies, these attacks violate integrity by modifying network traffic (El-Rewini, Sadatsharan, Selvaraj, et al., 2020; El-Rewini, Sadatsharan, Sugunaraj, et al., 2020). Ethernet commonly used address resolution protocols, that is, ARP and DHCP are the focus of these attacks. The adversary can forward ARP replies to attain network traffic and respond to DHCP server requests for network traffic control. These activities are key indicators of man-in-the-middle attacks that divert network traffic to the adversary for information theft and tempering (Chowdhury et al., 2020). Moreover, traffic integrity attacks also include session hijacking attacks. In a hijacking attack, entities spy to determine the Ethernet protocol's session information, participating as one endpoint of the session or altering the session.
- Control override attacks: The control override attack is a holistic attack that nulls and voids authentication. It enables an attacker to override the legitimate driver's commands and corrective action. There are security risks associated with Android OS-based telematics systems that enable legitimate users to execute different commands using low-speed CAN remotely (Jo et al., 2017). Moreover, an attacker can download over-the-air (OTA) firmware, alter the code to enable remote operating functionality or GPS tracking, and then re-distribute the altered firmware.
- In-vehicle network access attacks: This attack is associated with breaching safety by malicious device attachments. For example, attackers can plug an external device into the OBD-II port to obtain vehicular network access. The safety of OBD-II ports is extremely important as a malicious connection to the OBD-II port allows an attacker to access diagnostic information and unauthorized entry to the in-vehicle network enabling him to insert malicious code of his choice (Carsten et al., 2015). Valasek and Miller (2014) demonstrated such scenarios over CAN employing an ECOM cable and other connectors.
- Dongle exploitation attacks: The dongles inserted into the OBD-II port also pose a serious threat to the vehicular system as they can be controlled remotely (Hashem Eiza & Ni, 2017). A practical demonstration of such a case was the Bosch Drivelog connector dongle which provided several add-ons like tracking vehicle maintenance and guiding the driver to appropriate service locations. The Argus Cybersecurity firm carried out a brute-force attack capable of hacking this dongle connected to a OBD-II port. The shown capability of this attack is unauthorized access via Bluetooth, malicious communications over the controller area network, and engine failure of a traveling vehicle.

A summary of cyberattacks on intra-vehicle networks and countermeasures is given in Table 3.

TABLE 3 Summary of cyberattacks on intra-vehicle network and countermeasures.

Network protocol	Topology	Security level	Usage	Cyber threats	Countermeasure
CAN	Bus	High	Engine control and transmission unit (ECU), OBD-II interface, temperature control, body control modules, telematics, electronic controls	(Carsten et al., 2015; Choi, Joo, et al., 2018; Liu, Zhang, et al., 2017; Mousa et al., 2016)	(Choi, Jo, et al., 2018; Groza & Murvay, 2018; Liu, Zhang, et al., 2017; Tashiro et al., 2017)
LIN	Linear bus	Low	Temperature sensing, sunroof control, battery monitoring, Body control such as seats, windows, door locks, airflow, lighting and wipers, electronic control units (ECUs)	(Deng et al., 2017; Jadhav & Kshirsagar, 2018; Takahashi et al., 2017)	(Takahashi et al., 2017)
FlexRay	Bus and star	Medium	Time-triggered communications, broadcast network, x-by-wire system, high data rate	(Gu et al., 2016)	(Kishikawa et al., 2019)
MOST	Ring	Medium to high	Entertainment through audio, video and voice, mobile office	(Deng et al., 2017)	(Wolf et al., 2006)

2.3 | Inter-vehicle/V2X threats

V2X refers to all sorts of vehicular communications, such as V2V, V2I, Vehicle to Pedestrian (V2P), Vehicle to Network (V2N), and Vehicle to Cloud (V2C). V2X is defined in 3GPP standards, which include cellular (LTE Uu) and direct communication (LTE PC5; Li et al., 2018). In the case of an inter-vehicular communication scenario, potential attack sites mentioned by Petit and Shladover (2014) are elaborated here as follows. (1) Infrastructure: since cooperative CAVs can do V2I communications, such as smart parking systems, roadside communication units, and smart traffic signals, attacks on infrastructure exposes these vehicles to cyber threats. (2) Other CAVs: a hacker can also use some other cooperative autonomous vehicles to send false signals or information to the autonomous vehicle. (3) Anywhere: a hacker can attack a cooperative autonomous vehicle from anywhere, for example, from any conventional network connected to a vehicular network via the Internet. Some threats fall under the category of high threats, such as manipulation of map databases and sending fake/false signals, for example, sending wrong information from other CAVs or smart infrastructure, which demands the vehicle to apply brakes suddenly and can cause danger to the life of a passenger in the car. Wireless connectivity creates another opportunity for attackers to do malicious and harmful activities such as getting private information, for example, vehicle's position, and performing fake software or firmware updates for onboard sensors and embedded systems of a vehicle remotely. All of these kinds of vulnerabilities fall under the category of remote access vulnerabilities (Wyglinski et al., 2013). Now, we will discuss different attacks on inter-vehicular communications one by one.

2.3.1 | DoS attacks

The DoS attack is one of the basic attacks in vehicular ad-hoc networks (VANETs) that involves overwhelming a host with a huge amount of information to overload its resources inhabiting it from accepting or processing incoming information. The attacker normally sends multiple messages to the roadside unit, which overloads it and blocks all possible communications to legitimate users (Dibaei et al., 2020). The roadside units (RSUs) are multi-role components of

vehicular networks responsible for authentication, management, and updating vehicles. The DOS attack can be launched either by utilizing a single IP address, ordinarily from a single vehicle, or by using multiple IP addresses simultaneously in the distributed manner dubbed distributed denial of service (DDoS) attacks (Sheikh et al., 2020). DDoS attacks are more difficult to alleviate because the messages can arrive from many vehicles.

2.3.2 | Black-hole attacks

A black hole is a major security threat by which an attacker interrupts an effective route of data transportation by dropping packets rather than forwarding them to their target node, thus forming a black hole effect (Gautham & Shanmughasundaram, 2017). A similar attack is a gray hole in which a spiteful node just drops packets from some particular node or a percentage of packets in the network and forward other packets to their target address. Similarly, a node can create a gray hole by sometimes dropping the packets and then acting as normal. That is difficult to detect as the previous malicious node starts behaving normally now (Verma et al., 2015).

2.3.3 | Replay attacks

Replay attacks can also be considered as a type of man-in-the-middle attacks in which the attacker imitates himself as a legitimate user or as RSU and replays a valid transmission. Replay attacks target the authenticity and confidentiality of the system as the attacker hijacks a message between an RSU and a CAV holding the encryption key or password that empowers the intruder to authenticate itself in the future. The replay attacks are difficult to mitigate effectively, as a network entity does not know if it is under attack (Dibaei et al., 2020; Mishra et al., 2016). Moreover, the attacker's high mobility and packet integrity make detection more complex.

2.3.4 | Sybil attacks

In the Sybil attack, a hostile node represents itself as "multiple nodes" to have a stronger influence on the network. This is a type of masquerade attack that can be applied in vehicular networks to divert traffic in a certain direction (Dibaei et al., 2020; Mishra et al., 2016). This attack creates wrong road congestion information, which can encourage other vehicles to alter their routes to skip the congested areas. In CAV networks, the Sybil attacks are conducted with the aid of GPS spoofing attacks to assign a congestion-free route to certain vehicles, severely harming network topology.

2.3.5 | Malware

Vehicles regularly communicate with other users and the roadside unit for efficient driving. Moreover, the vehicular software and application unit need frequent updates from the RSU, and vehicles must guarantee that the updates they receive originate from a trusted source. When malware is installed into the RSUs, attackers can penetrate the VANETs to disrupt their normal functionality (Al-kahtani, 2012). Attacker-controlled RSU leads to severe malware infections, compromise of personal information, and a cause of serious malfunctions (El-Rewini, Sadatsharan, Selvaraj, et al., 2020; El-Rewini, Sadatsharan, Sugunaraj, et al., 2020). The most straightforward way to counter malware attacks is to introduce a firewall or a reputation-based protection system that guarantees that only messages from trusted sources are admitted (Zhang et al., 2014).

2.3.6 | Falsified-information attacks

Attacking nodes can advertise wrong information about congestion or road accidents to persuade other CAVs to deviate to alternate routes (Sheikh et al., 2020). Moreover, a trustworthy vehicle can become a malicious node and send fake messages anytime for personal benefits (Kerrache et al., 2016). Similarly, a rogue node can also build congestion by

ignoring to notify excess traffic or accidents on the road for malicious purposes. This attack type is usually combated by employing Hashing, asymmetric cryptography, and reputation-based schemes.

2.3.7 | Timing attacks

In this attack, a hostile node disturbs live updates and information exchange between RSUs and CAVs. The rapid entry and exit of vehicles in and out of networks introduce time synchronization constraints. The attacking node alters the time slot of the received packet to create an intentional synchronization error. The delay can lead to a major accident as the victim's vehicle gets the message very late than expected. The data transmission at fixed rates (Cencioni & Pietro, 2008) and cryptographic solutions such as Trusted Platform Module (TPM; Guette & Bryce, 2008) can be adopted to counter such attacks.

2.3.8 | Impersonation attacks

In an impersonation attack, a malicious node declares itself as an authorized RSU to deceive users and expose their authentication information. The malicious nodes can launch these attacks either to disturb the network or to gain access to network privileges. Moreover, rogue nodes could also impersonate other vehicles for personal gains, such as impersonating an emergency vehicle to get a higher priority within the network leading to lower congestion. Identity compromise or invalid attribute possession provokes these attacks, so Trust Authority (TA) and a Public Key Infrastructure (PKI; Chim et al., 2011) can be helpful in prevention.

2.4 | Inter-vehicle/V2X cyber defense

Much research has been conducted recently to safeguard CAVs against V2X and vehicle-to-cloud cyberattacks and will be discussed in this section. We summarize the recent and some conventional attack surfaces as well as countermeasures under V2X and V2C frameworks in Table 4.

The countermeasure techniques against cyberattacks are usually based on adaptive cruise control, observer-based estimation, Kalman filtering, deep learning techniques based on convolution neural networks, and long short-term memory-based encoders. The most prevalent communications for CAVs are V2V, in which vehicles use semi-autonomous adaptive cruise control (SA-ACC) to communicate with immediately preceding vehicles. This type of communication is always under threat of false-data injection and DoS attacks. Jeon et al. (2020) developed an observer-based estimation algorithm that can detect attacks while at the same time monitoring the health of RADAR sensors. The proposed control strategy achieves resilience against attacks or detected sensor faults by switching to a non-connected controller. A similar study was conducted by Van Wyk et al. (2019) for sensor anomaly identification and detection using a combined convolutional neural network (CNN) and Kalman filter-based X^2-detector resulting in high accuracy, sensitivity, and F1 score. Ashraf et al. (2021) and Hossain et al. (2020) used the long-short-term memory (LSTM) autoencoder technique which is a recurrent neural network (RNN) architecture. In this article, the authors presented a deep learning-based intrusion detection system to detect suspicious network events and intrusive activity of in-vehicles networks (IVN) such as CAN and external communication through V2V and V2I networks. Two benchmark datasets were used for simulation, the car hacking dataset for in-vehicle communications and the UNSW-NB15 dataset for external network communications. The proposed integrated architectures resulted in 98% and 99% overall accuracy for internal and external networks on the two datasets. Cyberattacks including DoS, gear, and RPM gauge spoofing, sniffing, fuzzy, and replay attacks can be detected using this design.

In VANET, a car is modeled as a mobile node using communication technologies such as 802.11p and cellular networks of 4G and 5G. The current VANET model against cyber threats is based on intrusion detection, prediction, and reaction system. There is a lot of communication overhead, for example, when there are more than 300 vehicular nodes. This could affect V2X communication and threaten the safety of passengers and cars. The hierarchical game approach was introduced by Sedjelmaci et al. (2018) against the lethal black hole, false data injection, and false dissemination attacks. In another investigation Hassan et al. (2020) proposed an intelligent black hole attack detection scheme tailored to autonomous and connected vehicles. Messages are skipped in black hole attacks, collected data from a vehicle sensor

TABLE 4 Summary of detection of cyberattacks on V2X in specific scenarios and control strategies.

Sensing channel	Risk scenario/attack type	Control scheme	Reference
V2V	RADAR sensor failure and cyberattack	Observer based semi-autonomous adaptive cruise control (SA-ACC)	(Jeon et al., 2020)
V2V and V2I	Sensor anomaly or cyberattack	CNN-KF based anomaly detection and identification	(Van Wyk et al., 2019)
In-vehicles networks (IVN), V2V and V2I	Denial of service, sniffing, distributed denial of service, spoofing and replay attacks	LSTM auto-encoder algorithm-based intrusion detection system (IDS), decentralized security exchange (DSE)	(Ashraf et al., 2021; Darby & Gottumukkala, 2019; Hossain et al., 2020)
VANET	Intrusion detection, prediction and reaction systems (IDS, IPS and IRS)	Cooperative game model	(Sedjelmaci et al., 2018)
Platooning with V2V	Denial of service	Observer based cooperative adaptive cruise control (CACC), biometric privacy, resilient distributed Kalman filter	(Abdollahi Biron et al., 2018; Amini et al., 2022; Amoozadeh et al., 2015; Dutta et al., 2020; Li, Lu, et al., 2019; Mousavinejad et al., 2020; Petrillo et al., 2020; Xiao et al., 2021; Zhang, Shen, et al., 2020)
V2V and V2I	Data Injection Attack on RADAR, IMU, LiDAR, Camera and roadside sensor	Multi-armed bandit algorithm for safe speed and distance between vehicles	(Ferdowsi et al., 2019)
In-vehicle CAN	Low-rate replay-based injection attacks	Subsequence mining-based anomaly detection	(Katragadda et al., 2020)
In-vehicle CAN-FD	Masquerade attacks	Message authentication codes	(Xie et al., 2020)
V2X (V2V, V2I, and V2R)	Distributed denial-of-service (DDoS)	Blockchain	(Li, Weng, et al., 2019)
VANET and SDN in IoV	Denial-of-service (DoS) and DDoS	Blockchain-secured fog computing, SVM classifier	(Gao et al., 2020; Yu et al., 2018)
Cognitive Radio Network (CRN) and IoV	Presence of Malicious Devices (MD)	CRT-BIoV: Blockchain-secured trust model based on technique for order preference by similarity to the ideal solution (TOPSIS)	(Rathee et al., 2020)
Cloud-assisted IoV	Internal and external sensors and communication channels	Cloud-assisted computing, AWS cloudlets	(Aladwan et al., 2020; Gupta et al., 2020a, 2020b; Jiang, Zhang, et al., 2020; Kim et al., 2020; Masood et al., 2020; Rathee et al., 2020; Shao & Wei, 2018; Sheik & Maple, 2019; Sun et al., 2019)

is modified, and wrong information is inserted in false data injection attacks. Similarly, a false dissemination attack spreads a false alert, thereby luring the authenticity of the vehicle about an accident and hence causing traffic jams. The system model proposed by Sedjelmaci et al. (2018) uses a fleet by varying the number of vehicles consisting of 300–700 nodes using a probabilistic mobility model generated by the Simulation of Urban Mobility (SUMO) simulator. The number of attackers varied from 10% to 30% of overall vehicles. Vehicles were clustered using agents. The hierarchical cooperative game was used as a system model. Cluster head agents interacted with secondary agents to predict and detect lethal attacks. The Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and Intrusion

Reaction System (IRS) are secondary players, and their approaches are to carry out the detection, forecast, and reaction actions, respectively. The Intrusion Decision Agent (IDA) is the leading player that is responsible for decisions in originating the plans of IDS, IPS, and IRS. The secondary and head agents collaborate to minimize the false positive and false negative rates while decreasing the processing delay and overhead.

Security vulnerabilities of CAVs and their impact on cooperative driving (platooning) were discussed extensively by several researchers (Abdollahi Biron et al., 2018; Amini et al., 2022; Amoozadeh et al., 2015; Dutta et al., 2020; Li, Lu, et al., 2019; Mousavinejad et al., 2020; Petrillo et al., 2020; Xiao et al., 2021; Zhang, Shen, et al., 2020), considering many different types of attacks, such as DoS and DDoS. Cooperative ACC is an extension of ACC that leverages inter-vehicle communications to create a tightly coupled vehicle stream. Security attacks on a Cooperative ACC vehicle stream consist of (a) falsification attack; (b) eavesdropping attack; (c) radio jamming attack; (d) tampering attack. Jamming attacks can cause a serious deadlock in car platooning. DoS, distributed DoS, and deception attacks are very popular for car platooning. Some countermeasures are proposed in the above-mentioned references. Observer-based Cooperative Adaptive Cruise Control, biometric privacy, and resilient distributed Kalman Filter are some notable control schemes. Fifth-generation communication systems aim at providing reliable, sustainable, and trustworthy networks with guaranteed quality of service. Software-defined networking (SDN) enabled 5G networks are designed to provide high data rates with low latency. Vehicular ad-hoc networks or VANETs will use 5G and emerging 6G technology to realize the Internet of Vehicles (IoV). Because of the security challenges in VANETs, trust among connected vehicles is a concern. SDN provides effective network management services. Blockchain is a decentralized, transparent, and immutable chain of transaction blocks designed to ensure trust in a networked world of autonomous vehicles. Being centrally controlled, SDN becomes vulnerable to DOS attacks and suffers from a single point of failure. Blockchain-enabled SDN will provide enhanced security against such attacks. Gao et al. (2020) utilized SDN-enabled blockchain for IoV in the 5G and fog computing system and proposed a trust system. Reputation scores were given to vehicles. Connected vehicles provide feedback about messages received by vehicles and authenticate and give verdicts about the connected vehicles. A similar and closely related work by Rathee et al. (2020) provided security to IoV during cognitive radio spectrum sensing and information transmission using cognitive radio network (CRN) by sensing the channels through a decision-making technique known as Technique for Order Preference by Similarity to the Ideal Solution (TOPSIS), which evokes the trust of its cognitive users by analyzing some predefined attributes. Further, blockchain is maintained in the network to trace every activity's stored information. Another survey paper by Mendiboure et al. (2020) provides some of the future directions for the widespread deployment and integration of blockchain-enabled vehicular networks. This survey compares different blockchain technologies such as Bitcoin, Ethereum, and Hyperledger fabric and provides services for fog computing, vehicular delay-tolerant network (VDTN), vehicular cloud computing, crowdsourcing, carpooling and platooning.

Security and privacy challenges for connected vehicles in IoV using vehicular cloud computing (VCC) are discussed by several investigators (Aladwan et al., 2020; Gupta et al., 2020a, 2020b; Jiang, Zhang, et al., 2020; Kim et al., 2020; Masood et al., 2020; Rathee et al., 2020; Shao & Wei, 2018; Sheik & Maple, 2019; Sun et al., 2019). Cloud-assisted CAV is an emerging research area. A representative scheme for V2C is shown in Figure 4.

Cloud computing has revolutionized the computing regime because of efficient resource utilization through virtualization. VCC is a promising solution to ensure road safety and traffic flow management in real-time Intelligent Transport Systems (ITS) (i.e., alternative routes, navigation, synchronization of traffic lights, and intersection management). VCC can be divided into the physical layer, V2X network layer, and, then cloud layer. Cloud-supported CAV applications face the challenge of a more robust and secure authentication system. In this regard, Kumar, Ahmad, et al. (2021) and Jiang et al. (2018) conducted notable research by presenting a combination of biometrics with elliptic-curve cryptography-assisted authentication framework and integration of 3-factor authentication with non-interactive identity-based key establishment protocol, respectively. Bousselham et al. (2019) addressed the scalability issue in establishing trust by combining decoy technology and user behavior profiling. The challenge of securing cloud-supported CAV applications was addressed by Hegde and Manvi (2019) by presenting a novel key management protocol. Due to a huge three-tier challenge of enabling proactive security by overcoming the issues of authentication of CAVs, establishing trust relationships, and securing CAVs' cloud data and communications networks, a lot of investigations are still needed.

2.5 | Data mining based anomaly detection in CAVs

Data mining techniques can be useful in intrusion detection and malicious vehicle detection as well as for improving road safety and accident prevention. Data mining techniques provide a new opportunity that can be utilized to ensure

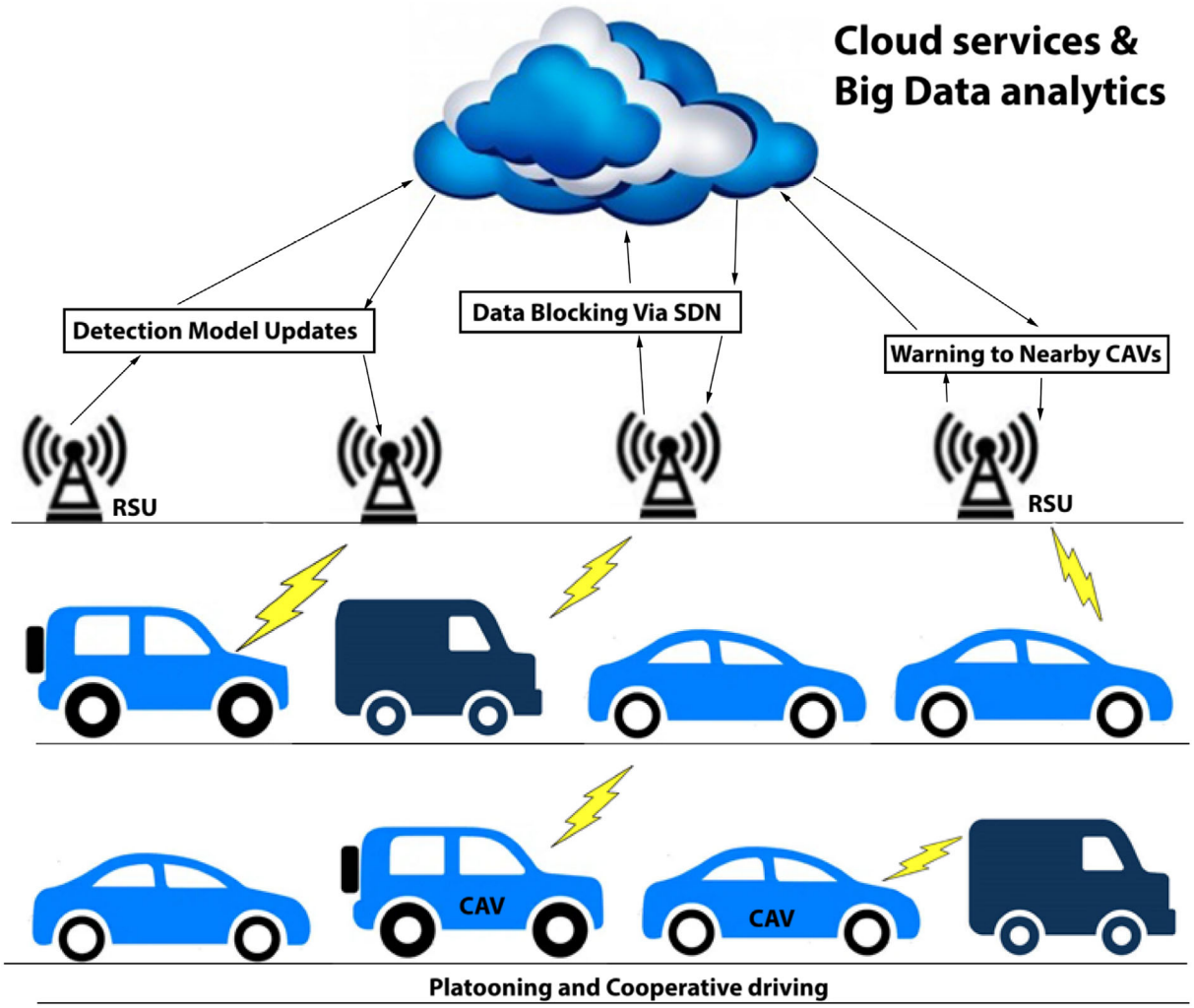

FIGURE 4 Cloud-assisted CAV.

safe driving by analyzing large volumes of vehicular data. These data mining techniques can also identify patterns and trends that may not be immediately apparent or visible, helping to identify risk factors and prevent accidents. Intrusion detection systems are a crucial part of security systems responsible for detecting and blocking an intrusion in an effective and timely manner. Several researchers have proposed the performance enhancement of intrusion detection systems using data mining techniques because of their higher efficiency and lower false alarms (Gudadhe et al., 2010; Sun et al., 2003). Data mining techniques can discover useful patterns of intrusion by applying statistics and inference theory to a CAV model. Two basic intrusion detection systems include misuse and anomaly detection systems, which can detect both known and unknown intrusions with unknown signature patterns, respectively (Depren et al., 2005).

CAV network relies on IEEE 802.11p standard which ensures vehicular safety as passengers travel toward their destination. CAV applications such as "Platooning" rely on cooperative awareness messages (CAMs) and a platoon-leading vehicle is responsible for making important decisions for the vehicle following platoon leader (Lyamin et al., 2014). The unreliability of V2V communications in a CAV-platooning application could seriously deteriorate the system-level performance and can also lead to life-threatening scenarios on roads. To address this issue, Lyamin et al. (2019) proposed a data mining-based radio jamming detection. The authors focused on various reasons for losses in CAM messages exchanged by vehicles in a platoon. These reasons for losses are based on knowledge of the IEEE 802.11p protocol rules and the historical observations of events in the V2V channel. This technique can be considered anomaly detection in a discrete sequence through data mining.

Another work by Rosell and Englund (2021) presented an efficient data aggregation mechanism for CAV network intrusion detection systems. This research enabled the extraction of frequency information from a window of CAN messages by using multiple datasets for various attack scenarios like flooding, fuzzing, and spoofing. The proposed method

successfully detects attacks and demonstrates the algorithm performance with linear models, support vector machine, and random forest, with the latter method yielding the best results (Park et al., 2021). Authors in He et al. (2020) pointed out the lack of a universal or broadly recognized framework for CAV cybersecurity. Based on the UK CAV cybersecurity principles, they have proposed a UML (Unified Modeling Language)-based CAV cybersecurity framework, that can classify potential vulnerabilities of CAV systems. As a result of this framework, a new CAV communication cyberattack data set (named CAV-KDD) is generated using an existing open-source data mining tool WEKA (Hall et al., 2009). CAV-KDD is based on the widely tested benchmark data set KDD99. The authors have further presented results of two classification models namely Decision Tree and Naive Bayes, based on this novel CAV-KDD training data set.

Concerning CAV's safety, Rezgui and Cherkaoui (2011) proposed a mechanism called VANETs association rules mining (VARM) for detecting faulty and malicious vehicles in VANETs. VARM collects data on each neighbor's transmission and extracts temporal correlation rules between vehicles in the neighborhood. The association rules derived from the mining process are used to detect a faulty or malicious vehicle that is not following these rules. The VARM scheme also employs a technique dubbed "1:N" to reestablish the accuracy of data collection between vehicles in the neighborhood, and the efficiency of the scheme is demonstrated through simulation results.

Park et al. (2021) discussed the issue of traffic safety related to rental cars and proposed a methodology for developing policies that can enhance safety. The study conducted an in-depth questionnaire survey of 781 corporate cab drivers and used data mining techniques to extract the intrinsic characteristics of cab drivers and classify them into four types. The derived policies were categorized into three groups: the development of new policies, the improvement of existing policies, and the elimination of negative factors. Authors in Lakshmi et al. (2022), discussed the need for effective monitoring of IoT devices to prevent cyberattacks. Additionally, the article proposed an alternative strategy to address the issue of unexpected traffic stops, particularly on fast-moving roads and motorways with restricted visibility, by installing mobile traffic sensors in individual and public vehicles.

Dias et al. (2023) proposed a tool to predict the risk of road accidents, which consists of the following steps: (a) data selection and collection, (b) preprocessing, and the use of mining algorithms. Data were collected from the Portuguese National Guard database and analyzed to understand the correlation between different variables that influence the frequency of accidents. This data-mining problem was approached as a regression problem, and the best result was achieved through the neural network. This work is of great benefit as it enables police to improve their future planning by predicting accident risk.

2.6 | Threats to software-updates and patching in CAVs

Software updates and patching play a crucial role in minimizing cybersecurity threats in connected automobiles. Regular updates allow for the detection and correction of vulnerabilities, thereby reducing the risk of successful cyberattacks. By keeping the software up to date, manufacturers can address known security concerns and implement necessary fixes to protect connected vehicles and their systems.

However, conducting software updates in connected vehicles requires careful consideration of security concerns. One major concern is the potential for malicious actors to exploit the update process itself as an entry point for attacks. To mitigate this risk, a safe way to conduct updates is to establish a secure and authenticated communication channel between the vehicle and the update server. This ensures that only authorized and verified updates are installed, reducing the possibility of unauthorized or tampered updates compromising the vehicle's security.

Additionally, secure over-the-air (OTA) update mechanisms can be employed (Park & Park, 2022; Nilsson & Larson, 2008; Zandberg et al., 2019), which encrypt the update packages and verify their integrity before installation. By implementing secure communication protocols and encryption techniques, the confidentiality and integrity of the update process can be maintained, safeguarding against potential attacks. Moreover, manufacturers should follow best practices in software development and security, including rigorous testing and vulnerability assessments before releasing updates. Regular monitoring and response to emerging threats and vulnerabilities are also essential to promptly address any new security risks that may arise.

Overall, the combination of regular software updates, secure communication channels, authenticated updates, encryption, and adherence to security best practices are vital in ensuring the end-to-end safety and security of connected vehicles (Evans et al., 2019) during the update process, thereby minimizing cybersecurity threats.

3 | MACHINE LEARNING FOR CAVS CYBERSECURITY

Machine learning algorithms can be used to detect potential cyberattacks in real-time by analyzing network traffic and system logs. Additionally, machine learning can be used to improve risk assessment and enhance situational awareness in autonomous vehicles.

A broad overview of ML approaches that can be utilized for cyberattacks in CAVs is given in this section. In the past decade, deep learning technology has been successfully applied to numerous applications, and among them, some applications are life crucial such as deep learning-aided CAVs (Sarker et al., 2020). This raises concerns in the security realm as great power associated with deep learning-aided design demands high responsibility (Yuan et al., 2019). One of the first investigations by Szegedy et al. (2013) revealed that DL models are vulnerable against well-crafted input samples, called "adversarial examples." These carefully designed samples can easily deceive a nicely working DL model with small changes termed as "perturbations" generally undetectable to humans. An adversarial example can be formally defined as "inputs to a deployed ML/DL model created by an attacker by adding an imperceptible perturbation in the actual input to compromise the integrity of the ML/DL model." In mathematical terms, an adversarial example can be written as

$$\overline{\mathbf{x}} = \mathbf{x} + \underset{\eta}{arg\,min}\{\| \eta \| f(x+\eta = t)\}, \tag{1}$$

where $\overline{\mathbf{x}}$ is an adversarial sample, $\mathbf{x}$ is the correctly classified sample, η is perturbation, $f()$ is the ML classifier, and t is the targeted class. Recent studies also suggest that adversarial examples can be employed to confuse autonomous vehicles by manipulating traffic signs or altering the segment of pedestrians in an object detection system (Xie et al., 2017). Several types of attacks are topics of extensive discussion in literature (Assion et al., 2019; Hafeez et al., 2019; Qayyum et al., 2020; Ren et al., 2020a, 2020b; Sadeghi et al., 2020; Sharma et al., 2019). Several adversarial examples generating methods will be discussed in the next subsection.

3.1 | Adversarial attacks

As discussed earlier, an input crafted in a specific way to obtain a wrong result from the model leads to an adversarial attack. Adversarial attacks that affect the training stage of the learning process are known as poisoning attacks (Jiang, Li, et al., 2020). The adversarial attacks that target the inference phase of a learning process are known as evasion attacks (Jiang, Li, et al., 2020). In evasion attacks, the adversary can manipulate either test samples or live inputs of given model for generating an incorrect result. Several more classifications of adversarial attacks based on adversarial knowledge, specificity, falsification, and attack frequency exist (Qayyum et al., 2020), however here we will focus on attack types and their countermeasures to enlighten the reader with a holistic overview of threats and defenses. Let us define some notations useful for describing adversarial attacks.

A dataset of size N is defined as $\{\mathbf{x}_i y_i\}_{i=1}^{N}$ with $\mathbf{x}_i$ and y_i being input samples and labels, respectively. The neural network in this case is represented by $f(.)$ which predicts a value of $f(x)$ based on input $\mathbf{x}$. The adversarial loss is denoted by $J(\boldsymbol{\theta},\mathbf{x},y)$ where $\boldsymbol{\theta}$ represents the model weights. In classification tasks, the cross-entropy loss function denoted by $J(f(x);y)$ is utilized. Moreover, the adversarial sample of $\mathbf{x}$ is denoted by $\overline{\mathbf{x}}$ and formulated as

$$\overline{\mathbf{x}} : D(\mathbf{x},\overline{\mathbf{x}}) < \eta, \quad f(\overline{x}) \neq y, \tag{2}$$

where $D(x)$ is the distance metric, η is the allowed perturbation that is practically taken as small as possible to guarantee the similarity between $\mathbf{x}$ and $\overline{\mathbf{x}}$.

3.1.1 | L-BFGS algorithm

The susceptibility of DNNs was first exposed by Szegedy et al. (2013) when they produced adversarial examples employing the L-BFGS method. The L-BFGS method finds the adversarial perturbations with the minimum L_p norm, which is expressed as

$$\min_{\mathbf{x}} = \|\mathbf{x} - \overline{\mathbf{x}}\|_p \; subject\, to f(\overline{x}) \neq \overline{y}. \tag{3}$$

Hardly perceptible adversarial perturbations are introduced by the L-BFGS attack to an image that can deceive the DNN and produce incorrect classification results. Szegedy et al. (2013) observed that the generated adversarial examples can be generalized to different models and datasets. Moreover, the usability of binary search to achieve the optimal perturbation for launching the L-BFGS attack was also investigated by Tabacof and Valle (2016).

3.1.2 | Fast gradient sign method

The time-consuming linear search constructed to obtain the optimal value in L-BFGS attack was addressed by Goodfellow et al. (2014), who first proposed the "Fast Gradient Sign Method" (FGSM) to generate adversarial examples. FGSM was fast, as indicated by its name, and could execute the one-step update toward the direction of the gradient of the adversarial loss $J(\boldsymbol{\theta},\mathbf{x},y)$, as well as follow the steepest direction toward the optimal value. The FGSM-generated adversarial sample can be expressed in mathematical terms as

$$\overline{\mathbf{x}} = \mathbf{x} + \varepsilon.sgn[\nabla_{\mathbf{x}} J(\boldsymbol{\theta},\mathbf{x},y)], \tag{4}$$

where ε represents the magnitude of the perturbation. FGSM can be manipulated to perform an attack by moving toward the slope of the gradient of the loss function $J(\boldsymbol{\theta},\mathbf{x},\overline{y})$, where $\overline{y}$ is the target label. The modified update rule for this type of attack can be written as

$$\overline{\mathbf{x}} = \mathbf{x} + \varepsilon.sgn[\nabla_{\mathbf{x}} J(\boldsymbol{\theta},\mathbf{x},\overline{y})]. \tag{5}$$

Another version of FGSM is the Fast Gradient Value method proposed by Rozsa et al. (2016) that replaces the sign of the gradient with the raw gradient, that is, $\eta = \nabla_{\mathbf{x}} J(\boldsymbol{\theta},\mathbf{x},y)$. The Fast Gradient Value method can produce images with a greater local difference and without any pixel constraints.

3.1.3 | Basic iterative method

The basic iterative method (BIM) is an extension of FGSM in which FGSM is applied multiple times with a small step size. In all iterations, clipped pixel values are used to prohibit large changes on each pixel. The BIM or Iterative-FGSM was explored by Kurakin, Goodfellow, and Bengio (2018), who generated adversarial examples closer to the original input as perturbations are added iteratively and hence have a greater chance of deceiving the network. The update rule of the t-th iteration can be written as follows

$$\overline{\mathbf{x}}_{t+1} = Clip[\overline{\mathbf{x}}_t + \alpha.sgn\{\nabla_{\mathbf{x}} J(\boldsymbol{\theta},\overline{\mathbf{x}}_t,y)\}]. \tag{6}$$

Three hyper-parameters required by the algorithm are per step perturbation α, maximum perturbation value, and the number of iterations (I). The Projected Gradient Descent (PGD) can be viewed as another variant of BIM that excludes the constraint $\alpha T = \varepsilon$. The PGD uses a smaller adversarial perturbation size with the following update procedure

$$\overline{\mathbf{x}}_{t+1} = proj\{\overline{\mathbf{x}}_t + \alpha.sign[\nabla_{\mathbf{x}} J(\boldsymbol{\theta},\overline{\mathbf{x}}_t,y)]\}, \tag{7}$$

where *proj* represents the projection operation of the adversarial sample to a valid range.

3.1.4 | Momentum iterative attack

Dong et al. (2018) realized that the one-step attack is easy to transfer but also relatively simple to defend and thus implements momentum to FGSM to produce adversarial examples with additional iterations. The new iterative

algorithm was dubbed the momentum iterative FGSM (MI-FGSM). Mathematically, MI-FGSM updates the adversarial sample iteratively as follows

$$\overline{\mathbf{x}}_{t+1} = Clip\left[\overline{\mathbf{x}}_t + \alpha.sgn\{\mathbf{g}_{t+1}\}\right], \tag{8}$$

where gradient g is updated according to

$$\mathbf{g}_{t+1} = \xi \mathbf{g}_t + \frac{\nabla_{\mathbf{x}} J(\boldsymbol{\theta}, \overline{\mathbf{x}}_t, y)}{\| \nabla_{\mathbf{x}} J(\boldsymbol{\theta}, \overline{\mathbf{x}}_t, y) \|}. \tag{9}$$

Dong et al. (2018) also presented the idea of considering the gradients of several models with respect to the input and finding a gradient direction that is more fit to transfer to other models.

3.1.5 | Distributionally adversarial attack

Zheng et al. (2019) investigated a distinct possible adversarial attack that takes the probability space into account and is dubbed "Distributionally Adversarial Attack (DAA)." Contrary to the PGD attack, which generates the adversarial samples independently for each data sample based on a loss function, the DAA applies optimization over the possible adversarial distributions. The suggested objective first involves the Kraft–McMillan (KL) divergence between the adversarial and benign data distribution in the evaluation of the adversarial loss. The distribution optimization problem can be expressed as

$$\max_{\mu} \int_{\mu} J(\boldsymbol{\theta}, \overline{\mathbf{x}}, y) \mathrm{d}\mu + \mathrm{KL}(\mu \overline{\mathbf{x}} \,\|\, \pi(x)), \tag{10}$$

where μ and $\pi(x)$ represents adversarial and non-adversarial data distributions, respectively. Compared with PGD, DAA investigates new adversarial patterns and is thought to be one of the most efficient attacks on multiple defensive models.

3.1.6 | Carlini and Wagner attack

Carlini and Wagner (2016) demonstrated that defensive distillation does not significantly increase the robustness of neural networks by introducing three new attack algorithms. A collection of optimization-based adversarial attacks are introduced by authors that can generate a set of norm-measured adversarial samples termed CW_0, CW_2, and CW_∞. The optimization objective can be expressed as

$$\min_{\delta} D(\mathbf{x}, \mathbf{x} + \boldsymbol{\delta}) + c.f(x + \delta), \quad \text{where } \mathbf{x} + \boldsymbol{\delta} \in [0, 1], \tag{11}$$

where δ denotes the perturbation, D represents the distance metric, and $f(x+\delta)$ denotes the specific adversarial loss that is true based on the condition $f(x+\delta) \leq 0$, provided that the attack target is predicted by the DNN. Further investigations by Carlini and Wagner (2017) revealed that C&W's attack is potent against most of the existing adversarial detecting defenses.

3.1.7 | Jacobian-based saliency map approach

Papernot, McDaniel, Jha, et al. (2016) designed an effective target attack termed JSMA that can deceive DNNs with small perturbations. The technique first calculates the Jacobian matrix of the logit (second-to-last layer) outputs. The Jacobian matrix of the sample $\boldsymbol{x}$ is

$$\nabla \mathbf{l}(\mathbf{x}) = \frac{\partial \mathbf{l}(\mathbf{x})}{\partial \mathbf{x}} = \left[\frac{\partial \mathbf{l}_j(\mathbf{x})}{\partial \mathbf{x}_\gamma}\right]_{\gamma \in 1...,M_{in} j \in 1...,M_{out}}, \tag{12}$$

where M_{in} and M_{out} are the number of neurons present in the input and output layers, respectively. γ and j are the indexes of input $\boldsymbol{x}$ and output l components, respectively.

The dilemma of how the elements of input $\boldsymbol{x}$ affect the logit outputs that are ready to be classified is addressed by the Jacobian matrix. In other words, the Jacobian matrix defines an adversarial saliency map that can select the pixels values that can be perturbed to obtain a certain change in logit outputs. As a result, the perturbations on a small proportion of elements that can affect the logit outputs can easily fool the neural network.

3.1.8 | DeepFool

DeepFool is an algorithm proposed by Moosavi-Dezfooli et al. (2016) to discover the closest distance from the original input to the decision boundary of adversarial examples. This algorithm encompasses an affine binary classifier and a general binary differentiable classifier. First, the authors established that the minimal perturbation of an affine classifier is the distance to the separating affine hyperplane

$$F = \left\{\mathbf{x} : \mathbf{w}^T\mathbf{x} + b = 0\right\}. \tag{13}$$

The perturbation of an affine classifier f can be expressed as $-\frac{f(x)}{\|w\|^2}w$. Second, for a general differentiable classifier, DeepFool treats F as linear around $\overline{x}_t$ and iteratively calculates perturbation $\boldsymbol{\delta}_t$ as

$$\underset{\boldsymbol{\delta}_t}{argmin} \parallel \boldsymbol{\delta}\parallel_2 \quad \text{subject to} f(\overline{x}_t) + \nabla f(\overline{x}_t)^T \boldsymbol{\delta}_t = 0. \tag{14}$$

This result can also be validated to a multi-class classifier by locating the closest hyperplanes and finding more general l_p norms. Investigations on the DeepFool algorithm revealed that the perturbation interjected by DeepFool is smaller than FGSM and JSMA on several benchmark datasets.

3.1.9 | GAN-based attacks

Pioneering work in the formation of adversarial samples with the generative adversarial network (GAN) was conducted by Xiao et al. (2018). Let us briefly introduce generative adversarial networks before discussing the loss model and other details. Given a big dataset, the GAN can generate brand-new unique data that is effectively indistinguishable from the original. The two core components of GAN are a generator and a discriminator. A generator makes new instances of an object, while the discriminator discovers whether the new instance belongs to the original dataset. The generator receives feedback from the discriminator and applies it to compose images that are more "real."

Let the generative adversarial networks comprising neural networks be Generator network G and a Discriminator network D. Moreover, let the real data distribution be P_{data}, the noise vector input to the generator be z that is taken from distribution P_z, whereas the generated samples are termed $G(z)$. Let the discriminator be a binary classifier that uses the real and synthesized samples as input and computes the probability of the sample being real. The training process of a GAN relates to the solution to the optimization problem introduced by Radford et al. (2015).

$$\underset{G}{min}\,\underset{D}{max} V(D,G) = \underset{\mathbf{x}\sim P_{data}}{E}[\log(D(\mathbf{x}))] + \underset{\mathbf{z}\sim P_z}{E}[\log(1 - D(G(\mathbf{z})))], \tag{15}$$

where $V(D,G)$ is the objective function, $D(\boldsymbol{x})$ denotes the probability that D discriminates $\boldsymbol{x}$ as real data, $G(\boldsymbol{z})$ is the sample generated by the generator, and $D(G(\boldsymbol{z}))$ indicates the probability that D determines the sample created by generator $G(\boldsymbol{z})$. There are several variants of GANs proposed after the initial work, such as the Conditional Generative

Adversarial Net (CGAN; Mirza & Osindero, 2014), Auxiliary Classifier GAN (AC-GAN; Odena et al., 2017). The research contribution of Arjovsky et al. (2017) and Gulrajani et al. (2017) is notable concerning training performance improvement.

3.1.10 | Universal adversarial attack

Generally speaking, any attack is crafted adversarial perturbation specific to certain benign samples. Since adversarial perturbations do not transfer across benign samples, some researchers have shown keen interest in finding a universal perturbation that can mislead the network on most benign samples. The initial work by Moosavi-Dezfooli et al. (2017) attempts to identify such a perturbation vector by iteratively updating of the perturbation employing all the target benign samples. Considering the benign samples that the present perturbation cannot deceive in an iteration, Moosavi-Dezfooli et al. (2017) proposed an algorithm for finding such perturbations whose goal is to find the minimum additional perturbation needed to compromise the samples. Furthermore, the additional perturbation is then joined to the present perturbation. At last, a perturbation can be found that deceives the network on most of the benign samples. There are several universal adversarial perturbations (UAP) techniques proposed by researchers, such as Vanilla Universal Attack (Moosavi-Dezfooli et al., 2017), SV-UAP (Khrulkov & Oseledets, 2018), network for adversary generation (NAG; Mopuri et al., 2018), and F-UAP (Zhang, Benz, et al., 2020).

3.1.11 | Adversarial patch

Perturbations in a confined region/segment of the benign samples are called adversarial patches. A carefully crafted adversarial patch can easily fool a DL model. For example, Sharif et al. (2016) discovered that state-of-the-art face recognition systems can be fooled by generating accessories like eyeglass frames. Adding to this context, Parkhi et al. (2015) showed venerability of usually used adversarial loss, such as cross-entropy, when the locally generated perturbation is used to deceive the VGG-Face convolutional neural network. Brown et al. (2017) suggested that a neural net can be fooled by completely replacing a part of an image with their designed patch. Liu et al. (2019) presented a black-box adversarial patch termed D-PATCH that can simultaneously attack the bounding box regression and object classification. Moreover, Athalye et al. (2017) presented expectation over transformation (EOT), a general-purpose algorithm for creating robust adversarial examples that can successfully fabricate three-dimensional adversarial objects. The investigation by Liu, Ma, et al. (2017) proposed appending a Trojan patch to benign samples to create adversarial samples.

3.1.12 | Miscellaneous attacks

The basic types of attacks are discussed in the previous section in the interest of space. There are several more variations of attacks by which adversarial samples can be created, such as Obfuscated-gradient circumvention attacks (Athalye et al., 2018), Elastic-net attack (Chen et al., 2018), Hot/Cold (Rozsa et al., 2016), CPPN EA Fool (Nguyen et al., 2015), Model-based Ensembling Attack (Liu, Chen, et al., 2017), and Ground-Truth Attack. There are several concerns about the application of some of these attacks, such as destruction of adversarial perturbations by environmental noise and natural transformations as well as perturbation being non-applicable to the image background.

3.2 | Defense against adversarial cyberattacks

Ensuring the overall defense of connected vehicles relies heavily on maintaining robust security mechanisms. With the increasing connectivity and integration of software and data-driven features, vehicles depend on databases to handle vast amounts of information. These databases hold sensitive data, including personal information, vehicle telemetry, and navigation history; therefore, their security must be guaranteed (Xia et al., 2022). To safeguard this valuable data and preserve privacy, the following measures should be implemented.

- Implement robust access control mechanism.
- Encrypt the data stored in the vehicle's database.
- Deployment of intrusion detection and monitoring systems.
- Secure database backup.
- Comply with privacy regulations.
- Regular auditing and testing of CAV database.
- Minimize the potential impact data breach utilizing distributed security mechanism.

We summarize the recent and some conventional adversarial defenses with a discussion on their types in Table 5.

Defense methods are designed based on two main approaches (Moosavi-Dezfooli et al., 2018; Wang et al., 2022), that is, (1) proactive approach, in which the target system is prepared for potential threats before the attack, and (2) reactive approach, which uses a defense technique after an attack. Most defense techniques rely on the first approach to prevent damage as much as possible.

3.3 | Adversarial versus conventional attacks

Adversarial attacks on connected and autonomous vehicles are a growing concern in the field of CAV cybersecurity. These attacks involve manipulating or deceiving the sensors, and algorithms associated with the deep learning modules of autonomous vehicles to cause malfunctions hereby, potentially leading to hazardous situations. To ensure CAV safety and train the DL modules to identify these attacks, it is important to provide critical analysis of adversarial attacks on connected and autonomous vehicles.

The adversarial attacks exploit vulnerabilities in perception systems, such as image recognition algorithms, LiDAR sensors, or RADAR systems, leading to false detection of objects on the road. The conventional attacks typically refer to attacks that exploit vulnerabilities in the vehicle's software or communication systems possibly leading to accidents or dangerous maneuvers. The field of CAV cybersecurity continuously evolves as new attack vectors emerge, technology advances and vulnerabilities are discovered. As the conventional and adversarial attacks target different dimensions of CAV we cannot neglect either one to ensure a fool-proof CAV security system. It is challenging to claim that all possible attacks have been exhausted, researchers and practitioners in the field of CAV cybersecurity strive to develop comprehensive frameworks that encompass a wide range of potential attacks and countermeasures. However, achieving absolute certainty that all attacks have been identified and addressed is a complex and ongoing task due to the evolving nature of cyber threats. Researchers and security experts often employ several methodologies such as threat modeling, vulnerability analysis, risk assessment, and penetration testing to identify and understand potential attack vectors. The frameworks developed by experts aim to cover a broad spectrum of attack possibilities, including conventional and adversarial attacks.

Another important consideration is the sophistication of adversarial attacks. As researchers have demonstrated, even subtle modifications to input data, such as adding imperceptible perturbations to images or modifying road signs, can deceive autonomous vehicles' perception systems. It is also important to note that defending against adversarial attacks is more challenging. It often requires developing robust and resilient perception algorithms that can detect and mitigate the impact of adversarial examples. Techniques like adversarial training, anomaly detection, and sensor fusion can help enhance the robustness of perception systems. Moreover, the adversarial attacks on autonomous vehicles have been demonstrated in research settings, there have been no major real-world incidents reported to date. However, the research community recognizes the importance of addressing this vulnerability proactively.

In conclusion, the collaboration between researchers, industry experts, and regulatory bodies is vital to establish best practices, standards, and regulations that can help mitigate the risks associated with conventional and adversarial attacks.

4 | CYBERSECURITY IN FEDERATED LEARNING ENABLED CAVS

Current and upcoming CAV systems feature a large number of devices that hold private data in conjunction with limited communication, computing, and storage resources that point toward a need for efficient utilization. Federated learning (FL) is an emerging approach that can be used to solve these challenges (Du et al., 2020). In this section,

TABLE 5 Defense against adversarial attacks.

Defense type	Defense strategies	Description	Related studies
Proactive	Adversarial training	Adding an adversary class to the training dataset containing adversarial samples. Common types are: • FGSM adversarial training • PGD adversarial training • Ensemble adversarial training • Adversarial logic pairing • Generative adversarial training	(Bai et al., 2017; Carlini et al., 2017; Engstrom et al., 2018; Goodfellow et al., 2014; Kannan et al., 2018; Kurakin et al., 2016; Xie et al., 2019; Zheng et al., 2016)
	Network distillation	Network distillation is commonly used to reduce the size of deep neural networks by transferring knowledge from a large network to a small one. It can also be utilized to protect deep neural networks against adversarial examples	(Hinton et al., 2015; Papernot & Mcdaniel, 2017; Papernot, McDaniel, Wu, et al., 2016; Soll et al., 2019)
	Classifier and model modification	This area includes several techniques that make classifier and model design robust. The domain includes: • Design robust classifier • Randomly choosing a classifier from a set to test each input to avoid classifier functionality theft • Aggregating multiple classifier outputs using ensemble methods • Combining kNN and DNN classifiers • Constructing a family of classifiers from the target classifier to be chosen randomly at test time • Change the architecture of the model to make it provably robust	(Abbasi & Gagné, 2017; Alabdulmohsin et al., 2014; Biggio et al., 2010; Biggio et al., 2015; Bradshaw et al., 2017; Lecuyer et al., 2019; Papernot & McDaniel, 2018; Raghunathan et al., 2020; Srisakaokul et al., 2018; Wong & Kolter, 2018)
	Model ensemble	Ensemble multiple models in order to make making the final prediction for improved robustness	(Kurakin, Goodfellow, Bengio, Dong, et al., 2018; Liu et al., 2018; Pang et al., 2019)
	Network regularization	A robust model is trained in this technique with an objective function that has a perturbation-based regularizer	(Cisse et al., 2017; Gu & Rigazio, 2014; Yan et al., 2018)
Reactive	Adversarial detection	In this technique a detector is utilized to trace adversarial examples or verifying the feature representation of inputs; moreover, hijacked images with triggers can also be traced	(Chen et al., 2019; Gao et al., 2019; Gu et al., 2019; Wang et al., 2019; Zheng & Hong, 2018)
	Adversarial transformation	These methods focus on such transformation that can convert adversarial examples back to clean images	(Guo et al., 2017; Jin et al., 2019; Liao et al., 2018; Samangouei et al., 2018)

we will conduct a brief review of studies on federated learning applied to CAVs. Google proposed federated learning (McMahan et al., 2017) for training a model in such a way that multiple parties can jointly participate in optimizing neural network parameters while simultaneously, minimizing privacy compromises. Federated learning offers privacy protections to the data located on the client side; however, in cases where dishonest clients or servers or both are present, the current FL system could also encounter security issues. The issue of ensuring a trust-worthy federated learning system that eliminates all possible threats is the focus of attention in academia and industry. The three core components of a federated learning system are: (1) Users that generate data and training models locally; (2) The FL system that furnishes a global model; and (3) A communication system for information exchange.

4.1 | Attacks on FL-enabled CAVs

A federated learning system that claims better privacy can be considered secure if it can also cope with malicious nodes' potential attacks and other security issues. The security issues posed by hostile nodes can delay the convergence process of a federated learning system and impact the accuracy of the trained model by a model poisoning process (Al Mallah et al., 2021). These federated learning deployment vulnerabilities in CAVs are explored by Al Mallah et al. (2021), and a number of attack scenarios like misleading the model by continuously driving through the same street or forging multiple identities by a single node, or sending a model trained on false data leading to a model poisoning attack were presented. Moreover, Al Mallah et al. (2021) adopted the FL protocol suggested by Bonawitz et al. (2019) for mobile networks and discussed the following attacks.

- Standard falsified information attacks: In these types of attacks, incorrect information is forwarded by a hostile vehicle that enters and exits a specific zone swiftly and thus continually sends fabricated real-time updates to the RSU. The zone under consideration characterizes the area where the RSU can receive messages. In this case, one hostile node generates adversarial local model updates and forwards them to the RSU to alter its model training. A malicious node aims to prevent the convergence of the global model. The standard falsified information attack provides maximum results with minimal effort because it can be launched with limited computational power. Furthermore, the mitigation of this attack is complex as the incoming messages may come from a legitimate and verified node. This cyber strike scenario can also be possible when a node forges the identity of a legitimate vehicle to launch a standard falsified information attack. An impersonation attack can benefit from a man-in-the-middle attack. The existing literature lacks the defense techniques that are specifically geared to deal with these situations.
- Sybil attacks: Sybil attacks can be considered an evolved version of the falsified information attack. In the Sybil attack, one vehicle fabricates another vehicle's identity to broadcast local model updates to alter the federated learning process. In this attack, the adversary node transmits multiple messages with distinct spoofed or stolen IDs. Thus the malicious node gains a substantial influence on the FL process. In every round of the federated learning protocol, a vehicle is randomly picked to participate in model training. A Sybil attack would allow the attacker to increase its chances of being selected to participate in training. More malicious vehicles' involvement in model training will damage the process and prevent the global model from convergence. A hostile node can simultaneously send falsified local model updates to perform a more severe attack via model replacement at convergence time. This design makes mitigation hard as it is virtually impossible to forecast a potential malicious behavior shown suddenly by several attacking nodes.

Attacks that mislead the FL process, such as Falsified information attacks, can degrade the performance considerably as FL depends on averaging to craft a global model. A malicious node seeks a more significant attack impact in a Sybil attack by creating multiple fake vehicle identities, simultaneously avoiding detection. This strategy is challenging for intrusion detection systems (IDS) to deal with compared to the attacks emanating from a single adversary; however, the Sybil attacks need to be carefully crafted, that is, traffic flow capacity and other demographics monitoring are necessary in order to avoid IDS detection.

4.2 | Defense against attacks on FL systems

The goal of hackers in the FL-based CAVs system is either to poison the model to disrupt the convergence or force the convergence to result in "sub-optimal" ineffective model. The defense techniques try to ensure a timely converged optimal model. The research literature of these defense strategies includes a secure aggregation mechanism for distributed learning to ensure convergence (Blanchard et al., 2017). Moreover, other designs use clustering to detect model updates that are different than normal ones. More recent solutions are designed to detect malicious nodes by evaluating information of the node's behavior (Kang et al., 2020). In this context, Driss et al. (2022) proposed a federated learning-based architecture in which a gated recurrent unit (GRU) is utilized for cyberattack detection. Moreover, Olowononi et al. (2021) proposed federated learning to protect data by keeping it local and differential privacy to strengthen the resiliency of CAVs to cyberattacks.

5 | BLOCKCHAIN-BASED CAVS SECURITY

Blockchain technology with its distributed ledger and cryptography enables faster and more secure data management. This efficient data management with blockchain enables self-driving cars to analyze and judge traffic in real-time, reduce accidents, identify best routes, and reduce travel time. The industry is facing several technical as well as legal challenges, including RADAR interference, driving in extreme weather conditions, and the current lack of necessary laws and regulations. Most autonomous cars use three technologies to navigate: LiDAR, cameras, and RADAR. Blockchain technology can be used to secure data transmission and storage in autonomous vehicles. By using blockchain, data can be stored in a tamper-proof and decentralized manner, which enhances data security and integrity. Blockchain is a distributed ledger that enables the recording of transactions and asset tracking. Blockchain can deliver numerous security benefits such as enhanced decentralized security, greater transparency, and instant traceability, thus facilitating an application to become cyberresilient (Akshay Kumaran et al., 2022; Kumar, Velliangiri, et al., 2021; Kumar, Wang, et al., 2021). Blockchain is a promising solution for making CAV communications secure and trustworthy. It keeps all transactions initiated in a CAV in the data blocks forming a chain-like structure. A transaction is added to the chain only after being authenticated by all blockchain network members. The network members keep a record of copies of a particular chain (Dargahi et al., 2021). In case of invalidation, the transaction append request is denied. A transaction can be any information about traffic, weather, or roadblock that a member of CAV can initiate.

Blockchain is a promising technique for decentralized applications, especially when mobile nodes or vehicles have a trust deficit due to relocation (Fraga-Lamas & Fernández-Caramés, 2019; Kumar, Wang, et al., 2021). The three essential components of a blockchain-enabled CAV network are data components, CAV networks, and transmission protocols.

Each block connects to the previous block utilizing hashes in blockchain-enabled CAV. Every hash is a specific value calculated by assessing block contents and used to detect errors. Blockchain technology includes the hash value of the preceding block to detect the tempering of any previous blocks in the chain. Any node that aims to send a block over the network must execute an algorithm termed Proof-of-Work (PoW; Fraga-Lamas & Fernández-Caramés, 2019), and then forward the solution to the network for approval. This prerequisite accomplishes two fundamental objectives: it prevents hostile nodes from sending inaccurate transaction data to the ledger, simultaneously restricting the total number of concurrent transactions that a ledger can accept to avoid overloading. In a CAV network, communications are independent of blockchain components. Vehicles generate detailed data requiring roadside nodes to set up a communication network regularly.

Blockchain technology addresses the fundamental problem of information transmission in CAVs, that is, security and trust. Existing trust models can be divided into entity-based, data-based, and hybrid trust (Kumar, Wang, et al., 2021). The entity-based trust models evaluate the trustworthiness of all contributing parties to decide if the blockchain is valid. The investigations by Gómez Mármol and Martínez Pérez (2012) as well as Gurung et al. (2013) proposed more systematic approaches for confirming the reliability of vehicles. All contributing nodes in a network are not reliable round the clock and can announce false data. High mobility negatively impacts the judgment of their trustworthiness. The entity-based trust models evaluate the trustworthiness of all contributing parties to decide if the blockchain is valid. Alternative to that approach is a "data-centric trust" model where vehicle's reliability is calculated based on their shared data. Investigations by Raya et al. (2008), and Gurung et al. (2013), evaluated a Bayesian inference decision module to estimate how truthful their reported events are. The past probabilities are taken into account in the inference module. A more secure approach is a hybrid trust framework used to evaluate trustworthiness by integrating entity-based trust and data-based trust. Adimoolam et al. (2021) introduced a trust-establishing technique that estimates the trustworthiness of data through the number of messages they receive from different nodes. There is a lot of research going on to overcome the inherent weaknesses of the hybrid trust system by improving the validation techniques and the reliability of messages and vehicles. The trend is to offer enhanced security by authorizing nodes to store trust levels on the blockchain (Cinque et al., 2020).

In the investigation by He et al. (2021), a blockchain-based federated learning framework dubbed "Bift" was investigated for connected and autonomous vehicles. To implement blockchain-based federated learning (BFL) systems, devices need to interface with decentralized servers with constrained communication and computation resources, impacting on the ML model training quality. Each device may be keen on participating in block mining to further gain blockchain rewards, for example, cryptocurrency tokens, which in turn enhance the reliability and security of FL. The article presents a popular Proof-of-Work mining mechanism for BFL, where participating devices compete against each other to become the first ones to solve the mining puzzle. Additionally, the work provides an efficient data-sharing architecture through InterPlanetary File System (IPFS), where experiments show that the IPFS-based data-sharing

system performs better than the traditional Secure File Transfer Protocol (SFTP). Moreover, Otoum et al. (2020) proposed an innovative solution involving a blockchain-based collective learning framework to ensure network security and data privacy are maintained. This framework is aimed at decentralizing the mutual machine learning models on end devices. To ensure that the shared cloud training can be trusted, a blockchain-based consensus solution is employed as a second line of defense and privacy protection. In this model, centralized training data and coordination are not necessary to enable end-device machine learning; this is achieved using a consensus method in blockchain. Otoum et al. (2020) also delegate the responsibility of storing ML models to a trusted community in the blockchain. Moreover, Krishna and Tyagi (2020) proposed a blockchain technology-based solution for detecting attacks and ensuring storage security. The research by Singh and Kim (2018) focused on guaranteeing security for broadcast data on the IoV by their proposed crypto Bit Trust that incorporates a reward-based system for communications.

In the paradigm of connected and autonomous vehicles, Fu et al. (2020) presented a decentralized ML learning framework, creating the possibility for vehicles to share the models, learn from each other, while ensuring privacy and security in the network. The investigation by Fu et al. (2020) proposed a blockchain-based collective learning (BCL) technique. The ML algorithms are used to improve the decision-making process of execution activities in the various layers of the IoV network, and the blockchain is applied to protect the users from security and privacy threats. Edge devices need to carry out the required task and determine time and energy utilization.

Leon Calvo and Mathar (2018) introduced a secure protocol for exchanging inter-vehicular messages based on blockchain. This implementation had the benefits of being decentralized and anonymous. Additionally, by utilizing the proposed platoon formation, which is the best in terms of road safety and efficiency, a ring-based signature scheme was used for authentication and to enable the vehicles to connect to the system. A blockchain technique that employs the multi-signature mechanism was presented by Lin et al. (2019). It offers evolving vehicular services such as remote software updates without disclosing any private information about the vehicles. In the investigation by Krishna and Tyagi (2020), the idea of having necessary security for IoT-based applications/systems was explained in the context of the IoV, which is a combination of IoT and mobile Internet. A blockchain-based Secure Storage Architecture for the Intelligent Internet of Vehicular Things (IIVoT) was developed by Das et al. (2020). In the research conducted by Taiyaba et al. (2020), a hypothetical framework that simulates the impact of difficult factors on blockchain implementation in the V2X paradigm was explained. There are a number of limitations that are associated with this like scalability issues, processing power and time, data protection, interoperability, and limited storage. Moreover, legal concerns and anonymity associated with such approaches are highlighted by Kapassa et al. (2021).

5.1 | Public and consortium blockchain-enabled CAV designs

Several investigators such as Baza et al. (2019); Dargahi et al. (2021); Kumar et al. (2022); Gupta et al., 2020a, 2020b Gupta et al. (2021), Rathee et al. (2019); Jain et al. (2021); He et al. (2021), provide a concise summary of blockchain-enabled CAV designs. Blockchain-enabled CAVs designs are divided into two main types that are commonly considered: public blockchain and consortium blockchain. Public blockchain refers to a decentralized network where anyone can participate and contribute to the blockchain's operations. It offers a high level of transparency and security but may come with scalability challenges due to the computational overhead required for consensus algorithms. Consortium blockchain, on the other hand, is a semi-decentralized network governed by a group of pre-selected participants. These participants usually represent organizations or entities involved in the CAV ecosystem, such as vehicle manufacturers, service providers, and regulatory bodies. Consortium blockchains offer a balance between decentralization and control, enabling efficient consensus mechanisms and higher scalability compared to public blockchains. When exploring research directions in blockchain-enabled CAV designs, it is crucial to consider the specific requirements and objectives of the application. Some potential research directions include:

Scalability and performance optimization: Developing novel consensus algorithms or improving existing ones to address scalability concerns in public blockchain implementations for CAV systems. This could involve techniques such as sharding, off-chain transactions, or layer-two solutions.
Privacy and data protection: Exploring techniques to ensure the privacy of sensitive data stored on the blockchain, such as implementing zero-knowledge proofs or secure multi-party computation. Additionally, research can focus on balancing the need for data transparency with privacy requirements in consortium blockchain setups.
Interoperability and standardization: Investigating protocols and frameworks that facilitate interoperability between different blockchain networks and CAV systems. This research direction aims to overcome the

challenges of integrating multiple blockchain platforms and ensuring seamless communication between CAVs and various stakeholders.

Smart contract applications: Exploring the potential of smart contracts in CAV systems to automate and enforce agreements between different parties. This could involve developing smart contract templates tailored for CAV-specific use cases, such as vehicle-to-vehicle communication, ride-sharing, or mobility service agreements.

Governance and regulatory considerations: Investigating mechanisms for governance and regulatory frameworks within blockchain-enabled CAV designs. This research direction explores the legal and policy aspects of blockchain implementation, addressing issues related to liability, accountability, and compliance.

By focusing on these research directions, scholars and practitioners can gain a deeper understanding of the challenges and opportunities presented by blockchain technology in the context of connected and autonomous vehicles. Such summaries help drive innovation, guide further research efforts, and inform the development of practical solutions for blockchain-enabled CAV systems.

6 | QUANTUM BASED SECURITY

Quantum computing has the potential to break traditional cryptographic algorithms, which could pose security challenges for securing data and communication in connected and autonomous vehicles. To address these challenges, several countermeasures can be considered:

1. Quantum-Resistant Cryptography: The algorithms that are resistant to quantum attacks should be adopted. These algorithms, often referred to as "post-quantum cryptography" (PQC) are specifically designed to withstand attacks from both classical and quantum computers. Examples include lattice-based cryptography, code-based cryptography, multivariate cryptography, and hash-based cryptography (Althobaiti & Dohler, 2021).
2. Quantum Key Distribution (QKD): Today's standard key exchange algorithms (such as Diffie-Hellman and RSA) are thought to be vulnerable to attacks by large-scale quantum computers. As such, there are two possible routes for avoiding this future threat: quantum-resistant algorithms (QRAs), such as those being developed under the National Institute of Standards and Technology (NIST) program, and quantum key distribution (QKD). Wright et al. (2021) utilized the principles of quantum mechanics to establish secure encryption keys between two parties. QKD ensures secure key distribution, even in the presence of quantum computers, providing strong protection for CAV communication. To make the complete V2X ecosystem quantum-safe, the following proactive measures should be considered.
   a. Implement standardized components such as quantum based random number generator (QRNG).
   b. Use postquantum (PQ) encryption algorithms.
   c. Apply QKD concepts.
   d. Use re-configurable hardware such as FPGA.
   e. However, it is important to note that so far the emergence of quantum computing and quantum resistant cryptography is not considered so far in context of protecting the V2X ecosystem end-to-end. 5G network slicing, software-defined networking and network function virtualization technologies can be used for CAV to dynamically control the type of encryption.
3. Hybrid Cryptography: A combination of classical and quantum-resistant cryptographic techniques should be employed to ensure enhanced security (Tangade et al., 2020). For example, a hybrid encryption scheme can utilize a classical algorithm for data encryption and a post-quantum algorithm for key exchange.
4. Quantum-Safe Transport Layer Security (TLS): TLS is widely used to secure communication over the internet. To make it resistant to quantum attacks, quantum-safe TLS protocols can be developed or adopted (Lokesh & Kaulgud, 2023). These protocols employ quantum-resistant key exchange algorithms and digital signatures to ensure secure communication between CAVs and backend systems.
5. Quantum Blockchain Technology: Blockchain provides a decentralized and tamper-resistant platform for secure data storage and communication. Implementing blockchain-based solutions can enhance the security of CAVs by ensuring data integrity, transparency, and immutability. Quantum-resistant cryptographic algorithms can be used within the blockchain framework to secure transactions and data (Fernández-Caramès & Fraga-Lamas, 2020; Yang et al., 2022).

6. Continuous Monitoring and Update: As quantum technologies evolve, it is crucial to stay informed about the latest advancements in quantum computing and cryptographic algorithms. Regularly assess and update the security measures in CAV systems to incorporate the most up-to-date countermeasures against potential quantum threats.

7 | CYBERSECURITY EMERGING TRENDS AND CHALLENGES

The research to date in the domain of securing vehicles against cybersecurity threats and possible attacks has addressed a number of security challenges and proposed many solutions. However, there are still open problems that need further investigation. In this section, we will illustrate some important and challenging problems and outline possible approaches and research directions to counter the hurdles in deploying a secure CAV network.

7.1 | Cybersecurity challenges and open issues

1. Adversarial resilience ML:

Deep learning algorithms have shown their high caliber in scene perception and object identification in autonomous vehicles. However, as discussed in Section 4, DL algorithms are prone to well-crafted adversarial attacks. Research has shown that such carefully crafted adversarial perturbations can deceive ML algorithms, wreaking havoc in CAV models due to their heavy reliance on ML and computer vision. Due to that imminent threat, the requirement for newer adversarial attack-resilient deep learning approaches and algorithms becomes more crucial. Due to the delicate nature of tasks assigned to CAVs (safe transportation of human beings), the development of deep learning frameworks with the following properties remains a challenging open research problem (Qayyum et al., 2020).

- Adversarially robust ML.
- Interpretable or explainable ML.
- Privacy-preserving ML.
- Robust ML against train/test drifts.

2. Federated learning associated challenges:

Federated learning has proven to be a promising approach for data privacy in connected and autonomous vehicles. Edge devices, that is, vehicles, hold training data, and therefore CAV network has a highly non-uniform data distribution. The increased data diversity from the sea of vehicles causes large variances in the averaged gradient data resulting in a low convergence rate of learning models. A delay in the convergence process of a federated learning system severely impacts the accuracy of the trained model, causing a server response delay and a non-converged model that threatens a CAV system. Malicious nodes can also send misleading updates that lead to data poisoning attacks. That problem can be addressed by a federated learning-based framework for efficient cyberattack detection as proposed by Driss et al. (2022).

3. Trust models and blockchain-enabled security:

Trust is an important parameter to protect CAVs against various security threats. Vehicles communicate with each other based on the degree of trust. Trust in VANET depends upon the behavior of other neighboring vehicles. Existing security solutions may not be deemed fit against many cyberattacks, as mentioned in the previous sections. Blockchain technology is a viable solution to establish trust among CAVs, protecting data tampering, faster data access through distributed data ledger technology, (i.e., each participating member has a copy of all un-modifiable data or transactions), non-repudiation, activity monitoring, and no centralized point-of-failure. In an AI-centric IoV, distributed ledger/blockchain technology can provide AI data integrity via immutable records and distributed trust between different CAVs. A blockchain network (BN) stores transaction data generated by vehicles and roadside units in its blocks. However, transactions are added to blocks only if verified by members of the BN; otherwise, they are rejected. A transaction may contain traffic information, weather-related data, road infrastructure, and obstacles information. The BN requires

real-time high-performance computing, and CAVs do not have such capability. Developing efficient BNs is still in its infancy, and various research challenges exist, such as enabling large system throughput for various BN consensus algorithms, decreasing latency, scalability issues, trust in CAVs whether it uses a public BN or private BN, financial cost, and high energy consumption. Based on this brief discussion, it is evident that there is a lot of room for further development in both fields.

4. Cloud-supported CAVs cybersecurity:

Challenges related to the cybersecurity of cloud-supported CAVs are threefold as the security of such systems is dependent on CAVs, cloud, and communication protocols (Salek et al., 2022). Securing data associated with connected vehicles in the cloud is important as its breach compromises multiple security requirements necessary for proper CAVs functionality, for example, confidentiality and integrity. The communication side challenges are associated with the authentication of high mobility nodes and the scalability of cybersecurity protocols. Generally, CAVs enter and exit the limited range of access points in a short time interval. At the same time, massages-based authentication is difficult to establish when the network topology is continuously changing. Moreover, in unreliable wireless communications scenarios where the probability of packet loss is high, the working of authentication protocols that utilize the exchange of tokens, such as passwords and signatures, becomes problematic. Authenticating a large number of CAVs in real-time is another cybersecurity challenge, especially in cases of multihop routing, as CAVs communicate with the cloud through several (depending on the network topology) intermediate nodes, for example, other CAVs, and RSUs. In such cases, the cloud needs to authenticate all the intermediate nodes, which adds to the computational complexity and difficulty in the operation of real-time applications.

5. Quantum-safe security:

Cybersecurity researchers are concerned that novel computers based on quantum physics rather than more standard electronics could break most modern cryptography. Fortunately, the threat so far is questionable. The quantum computers that exist today cannot annihilate any commonly used encryption methods. Notable technical advances are required before they can crack the strong codes in widespread use on the Internet. V2X communication must provide road safety, traffic capability, and energy savings, including all its variants, such as V2I, V2N, V2C, V2V, and V2P. Advances in computing and communication technologies drive the adoption of these technologies, and the CAV industry must also defend itself against an evolving threat landscape and the impending quantum age by researching quantum-safe security solutions such as IDQ's Quantum Key Distribution (Quantum Cryptography), Quantum Key Generation and Quantum-Safe Network Encryption solutions offering unmatched protection of information. The danger posed by future quantum computers still concerns information security today—the “download now, decrypt later” attack vector means that (encrypted) sensitive data can be downloaded today and analyzed offline when a quantum computer develops. Combining post-quantum cryptography techniques with physical layer security schemes may ensure secure 6G communication links. Combining ML physical layer cybersecurity and quantum encryption in 5G or 6G networks may enhance the overall security of CAVs against unpredictable future attacks.

6. Proactive defense of CAVs:

Several types of adversarial attacks introduced in Section 4 demonstrate the vulnerability of machine learning modules in CAVs. However, the defense strategies are relatively sparse and revolve around implementing new attacks and improving the training of ML models accordingly. In comparison, less attention was given to a defense framework and improving the robustness of ML models. Recently some studies, such as Gürel et al. (2021), focused on implementing a general defense framework to address the vulnerability posed by adversarial ML. Moreover, Gürel et al. (2021) proposed “Knowledge Enhanced Machine Learning Pipeline (KEMLP),” a framework to enhance the ML robustness utilizing domain knowledge.

Deep learning-assisted CAVs is considered one of the gigantic data-generating fields as DL model performance relies on the training dataset's size. However, ML data security is also neglected in the industry and academia. Improving the security of the training and test data is essential as CAVs control and decision-making rely on these datasets. Currently, the data generated by CAVs is stored in a distributed manner, which is prone to attacks and raises concerns about the soundness of these datasets. The domain of federated learning-enabled CAVs mostly suffers from poisoning

attacks, hence, sophisticated defense strategies are needed that can provide guarantees against these threats. Specifically, security mechanisms based on encryption, localization, behavioral analysis, and clustering can be promising for detection and evading poisoning attacks.

7. Cybersecurity protocols standardization:

Another important challenge is the standardization of cybersecurity protocols. The lack of a unified protocol across regions will increase complexity and interoperability. CAV cybersecurity systems must be tested before their deployment, however, there is no unified testing standard. As a result, each CAV manufacturer selects their own testing methods. Existing testing guidelines should be revised, taking all attack scenarios into account.

8 | CONCLUSION

Since the last decade, the research on vehicular communications and intelligent transportation systems has advanced rapidly. In order to securely deploy a network for CAVs, the defense mechanism against several cyber threats must be in place. This survey provides a comprehensive overview of cyberattacks on the sensing layer of CAVs in the context of intra-vehicle and inter-vehicle communication technologies. The study focused primarily on crossovers between communications, control, artificial intelligence, sensor fusion, and cybersecurity, where a system integrated approach in intelligent vehicles is seen in detail. In addition, this review conducts an in-depth study of communication analytics affecting traffic flow, use cases, security, and privacy in CAVs from conventional and machine learning perspectives. The hallmark of this article is the presentation of a holistic viewpoint on modern machine learning, federated learning and blockchain approaches in the context of CAVs. The survey also covers the recent and future challenges along with the guideline for cutting-edge technology and potential bottlenecks for a variety of use cases.

AUTHOR CONTRIBUTIONS

Jameel Ahmad: Investigation (lead); writing – original draft (lead). **Muhammad Umer Zia:** Investigation (lead); writing – original draft (lead). **Ijaz Haider Naqvi:** Investigation (equal); writing – review and editing (equal). **Jawwad Nasar Chattha:** Investigation (equal); supervision (equal); writing – review and editing (equal). **Faran Awais Butt:** Investigation (equal); writing – review and editing (equal). **Tao Huang:** Investigation (equal); supervision (lead); writing – review and editing (equal). **Wei Xiang:** Investigation (equal); writing – review and editing (lead).

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

ACKNOWLEDGMENT

Open access publishing facilitated by La Trobe University, as part of the Wiley - La Trobe University agreement via the Council of Australian University Librarians.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Jameel Ahmad https://orcid.org/0000-0003-4283-4946
Muhammad Umer Zia https://orcid.org/0000-0001-7621-4265
Ijaz Haider Naqvi https://orcid.org/0000-0001-8382-9217
Jawwad Nasar Chattha https://orcid.org/0000-0003-4444-6306
Faran Awais Butt https://orcid.org/0000-0002-4940-3842
Tao Huang https://orcid.org/0000-0002-8098-8906
Wei Xiang https://orcid.org/0000-0002-0608-065X

RELATED WIREs ARTICLES

Privacy-preserving data mining and machine learning in healthcare: Applications, challenges, and solutions

REFERENCES

Abbasi, M., & Gagné, C. (2017). *Robustness to adversarial examples through an ensemble of specialists*. arXiv: https://arxiv.org/1702.06856

Abdollahi Biron, Z., Dey, S., & Pisu, P. (2018). Real-time detection and estimation of denial of service attack in connected vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, *19*, 3893–3902.

Abreu, Z., & Pereira, L. (2022). Privacy protection in smart meters using homomorphic encryption: An overview. *WIREs Data Mining and Knowledge Discovery*, *12*, e1469. https://doi.org/10.1002/widm.1469

Adimoolam, M., John, A., Balamurugan, N., & Ananth Kumar, T. (2021). Green ICT communication, networking and data processing. In *Green computing in smart cities: Simulation and techniques* (pp. 95–124). Springer.

Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., & Leinmüller, T. (2006). Attacks on inter vehicle communication systems—An analysis. *Proceedings WIT*, *20*, 189–194.

Akshay Kumaran, V., Tyagi, A. K., & Kumar, S. (2022). Blockchain technology for securing internet of vehicle: Issues and challenges. In *International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–6). IEEE.

Al Mallah, R., Badu-Marfo, G., & Farooq, B. (2021). Cybersecurity threats in connected and automated vehicles based federated learning systems. In *IEEE Intelligent Vehicles Symposium Workshops (IV Workshops)* (pp. 13–18). IEEE.

Alabdulmohsin, I. M., Gao, X., & Zhang, X. (2014). Adding robustness to support vector machines against adversarial reverse engineering. In *Proceedings of the 23rd ACM International Conference on Information and Knowledge Management*. ACM.

Aladwan, M. N., Awaysheh, F. M., Alawadi, S., Alazab, M., Pena, T. F., & Cabaleiro, J. C. (2020). TRUSTE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud. *IEEE Transactions on Industrial Informatics*, *16*, 6203–6213.

Al-kahtani, M. (2012). *Survey on security attacks in vehicular ad hoc networks (VANETs)*. IEEE.

Almagrabi, A. O. (2023). Challenges and vulnerability evaluation of smart cities in IoT device based on cybersecurity mechanism. *Expert Systems*, *40*, e13113. https://doi.org/10.1111/exsy.13113

Althobaiti, O. S., & Dohler, M. (2021). Quantum-resistant cryptography for the internet of things based on location-based lattices. *IEEE Access*, *9*, 133185–133203.

Amini, A., Asif, A., & Mohammadi, A. (2022). A unified optimization for resilient dynamic event-triggering consensus under denial of service. *IEEE Transactions on Cybernetics*, *52*, 2872–2884.

Amoozadeh, M., Raghuramu, A., Chuah, C.-n., Ghosal, D., Zhang, H. M., Rowe, J., & Levitt, K. (2015). Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine*, *53*, 126–132.

Arjovsky, M., Chintala, S., & Bottou, L. (2017). Wasserstein generative adversarial networks. In *International Conference on Machine Learning* (pp. 214–223). PMLR.

Ashraf, J., Bakhshi, A. D., Moustafa, N., Khurshid, H., Javed, A., & Beheshti, A. (2021). Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, *22*, 4507–4518.

Assion, F., Schlicht, P., Greßner, F., Günther, W., Hüger, F., Schmidt, N., & Rasheed, U. (2019). The attack generator: A systematic approach towards constructing adversarial attacks. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (pp. 1370–1379). IEEE.

Athalye, A., Carlini, N., & Wagner, D. A. (2018). *Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples*. arXiv: https://arxiv.org/abs/1802.00420

Athalye, A., Engstrom, L., Ilyas, A., & Kwok, K. (2017). *Synthesizing robust adversarial examples*. arXiv: https://arxiv.org/abs/1707.07397

Axelrod, C. W. (2017). Cybersecurity in the age of autonomous vehicles, intelligent traffic controls and pervasive transportation networks. In *2017 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1–6). IEEE.

Axelrod, C. W. (2018). Cybersecurity and privacy issues when applying railway technologies to intelligent roadway systems. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)* (pp. 1–6). IEEE.

Bai, W., Quan, C., & Luo, Z. (2017). Alleviating adversarial attacks via convolutional autoencoder. In *18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)* (pp. 53–58). IEEE.

Batres, A. G., Moghe, A., & Taiber, J. (2016). A communication architecture for wireless power transfer services based on DSRC technology. In *IEEE Transportation Electrification Conference and Expo (ITEC)* (pp. 1–8). IEEE.

Baza, M., Nabil, M., Lasla, N., Fidan, K., Mahmoud, M., & Abdallah, M. (2019). Blockchain-based firmware update scheme tailored for autonomous vehicles. In *IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1–7). IEEE.

Bhat, A., Aoki, S., & Rajkumar, R. (2018). Tools and methodologies for autonomous driving systems. *Proceedings of the IEEE*, *106*, 1700–1716.

Biggio, B., Corona, I., He, Z.-M., Chan, P. P., Giacinto, G., Yeung, D. S., & Roli, F. (2015). One-and-a-half-class multiple classifier systems for secure learning against evasion attacks at test time. In *International Workshop on Multiple Classifier Systems* (pp. 168–180). Springer.

Biggio, B., Fumera, G., & Roli, F. (2010). Multiple classifier systems for robust classifier design in adversarial environments. *International Journal of Machine Learning and Cybernetics*, *1*, 27–41.

Blanchard, P., El Mhamdi, E. M., Guerraoui, R., & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent. In *Proceedings of the 31st International Conference on Neural Information Processing Systems, NIPS'17* (pp. 118–128). Curran Associates.

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Kiddon, C., Konečný, J., Mazzocchi, S., McMahan, H. B., Van Overveldt, T., Petrou, D., Ramage, D., & Roselander, J. (2019). *Towards federated learning at scale: System design*. arXiv: https://arxiv.org/abs/1902.01046

Bousselham, M., Benamar, N., & Addaim, A. (2019). A new security mechanism for vehicular cloud computing using fog computing system. In *International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)* (pp. 1–4). IEEE.

Bradshaw, J., Matthews, A. G. d. G., & Ghahramani, Z. (2017). *Adversarial examples, uncertainty, and transfer testing robustness in gaussian process hybrid deep networks*. arXiv: https://arxiv.org/1707.02476

Brown, T. B., Mané, D., Roy, A., Abadi, M., & Gilmer, J. (2017). *Adversarial patch*. arXiv: https://arxiv.org/abs/1712.09665

Carlini, N., Katz, G., Barrett, C., & Dill, D. L. (2017). *Provably minimally-distorted adversarial examples*. arXiv: https://arxiv.org/abs/1709.10207

Carlini, N., & Wagner, D. (2016). *Towards evaluating the robustness of neural networks*. arXiv: https://arxiv.org/abs/1608.04644

Carlini, N., & Wagner, D. (2017a). *Adversarial examples are not easily detected: Bypassing ten detection methods*. arXiv: https://arxiv.org/abs/1705.07263

Carlini, N., & Wagner, D. (2017b). *Magnet and "efficient defenses against adversarial attacks" are not robust to adversarial examples*. arXiv: https://arxiv.org/abs/1711.08478

Carsten, P., Andel, T. R., Yampolskiy, M., & McDonald, J. T. (2015). *In-vehicle networks: Attacks, vulnerabilities, and proposed solutions*. ACM.

Cencioni, P., & Pietro, R. (2008). A mechanism to enforce privacy in vehicle-to-infrastructure communication. *Computer Communications*, *31*, 2790–2802.

Changalvala, R., & Malik, H. (2019). Lidar data integrity verification for autonomous vehicle. *IEEE Access*, *7*, 138018–138031.

Chattopadhyay, A., Lam, K.-Y., & Tavva, Y. (2020). Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems*, *22*(11), 1–15.

Chen, B., Carvalho, W., Baracaldo, N., Ludwig, H., Edwards, B., Lee, T., Molloy, I., & Srivastava, B. (2019). *Detecting backdoor attacks on deep neural networks by activation clustering*. arXiv: https://arxiv.org/abs/1811.03728

Chen, P.-Y., Sharma, Y., Zhang, H., Yi, J., & Hsieh, C.-J. (2018). *Ead: Elastic-net attacks to deep neural networks via adversarial examples*. AAAI conference on artificial intelligence.

Chim, T. W., Yiu, S.-M., Hui, L. C., & Li, V. O. (2011). *SPECS: Secure and privacy enhancing communications schemes for VANETs* (Vol. 9, pp. 189–203). Elsevier.

Choi, W., Jo, H. J., Woo, S., Chun, J. Y., Park, J., & Lee, D. H. (2018). Identifying ecus using inimitable characteristics of signals in controller area networks. *IEEE Transactions on Vehicular Technology*, *67*, 4757–4770.

Choi, W., Joo, K., Jo, H. J., Park, M. C., & Lee, D. (2018). Voltageids: Low-level communication characteristics for automotive intrusion detection system. *IEEE Transactions on Information Forensics and Security*, *13*, 2114–2129.

Chowdhury, A., Karmakar, G., Kamruzzaman, J., Jolfaei, A., & Das, R. (2020). Attacks on self-driving cars and their countermeasures: A survey. *IEEE Access*, *8*, 207308–207342.

Cinque, M., Esposito, C., Russo, S., & Tamburis, O. (2020). Blockchain-empowered decentralised trust management for the internet of vehicles security. *Computers & Electrical Engineering*, *86*, 106722. https://www.sciencedirect.com/science/article/pii/S0045790620305772

Cisse, M., Bojanowski, P., Grave, E., Dauphin, Y., & Usunier, N. (2017). Parseval networks: Improving robustness to adversarial examples. In *International Conference on Machine Learning* (pp. 854–863). PMLR.

Cui, L., Xie, G., Qu, Y., Gao, L., & Yang, Y. (2018). Security and privacy in smart cities: Challenges and opportunities. *IEEE Access*, *6*, 46134–46145.

Darby, P., & Gottumukkala, R. (2019). Decentralized computing techniques in support of cyber-physical security for electric and autonomous vehicles. In *IEEE Green Technologies Conference (GreenTech)* (pp. 1–5). IEEE.

Dargahi, T., Ahmadvand, H., Alraja, M. N., & Yu, C.-M. (2021). Integration of blockchain with connected and autonomous vehicles: Vision and challenge. *Journal of Data and Information Quality*, *14*, 1–10. https://doi.org/10.1145/3460003

Das, D., Banerjee, S., Mansoor, W., Biswas, U., Chatterjee, P., & Ghosh, U. (2020). Design of a secure blockchain-based smart IOV architecture. In *3rd International Conference on Signal Processing and Information Security (ICSPIS)* (pp. 1–4). IEEE.

Deng, J., Yu, L., Fu, Y., Hambolu, O., & Brooks, R. R. (2017). Chapter 6—Security and data privacy of modern automobiles. In M. Chowdhury, A. Apon, & K. Dey (Eds.), *Data analytics for intelligent transportation systems* (pp. 131–163). Elsevier.

Depren, O., Topallar, M., Anarim, E., & Ciliz, M. K. (2005). An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks. *Expert Systems with Applications*, *29*, 713–722. https://www.sciencedirect.com/science/article/pii/S0957417405000989

Dias, D., Silva, J. S., & Bernardino, A. (2023). The prediction of road-accident risk through data mining: A case study from Setubal, Portugal. In *Informatics* (Vol. 10, p. 17). MDPI.

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., & Yu, S. (2020). Attacks and defences on intelligent connected vehicles: A survey. *Digital Communications and Networks*, *6*, 399–421.

Dong, Y., Liao, F., Pang, T., Su, H., Zhu, J., Hu, X., & Li, J. (2018). Boosting adversarial attacks with momentum. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 9185–9193). IEEE.

Driss, M., Almomani, I., Huma, Z., & Ahmad, J. (2022). A federated learning framework for cyberattack detection in vehicular sensor networks. *Complex & Intelligent Systems*, *8*, 4221–4235.

Du, Z., Wu, C., Yoshinaga, T., Yau, K.-L. A., Ji, Y., & Li, J. (2020). Federated learning for vehicular internet of things: Recent advances and open issues. *IEEE Open Journal of the Computer Society*, *1*, 45–61.

Dutta, R. G., Hu, Y., Yu, F., Zhang, T., & Jin, Y. (2020). Design and analysis of secure distributed estimator for vehicular platooning in adversarial environment. *IEEE Transactions on Intelligent Transportation Systems*, *23*, 1–12.

Eiza, M. H., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. *IEEE Vehicular Technology Magazine*, *12*, 45–51.

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications*, *23*, 100214.

El-Rewini, Z., Sadatsharan, K., Sugunaraj, N., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity attacks in vehicular sensors. *IEEE Sensors Journal*, *20*, 13752–13767.

Engstrom, L., Ilyas, A., & Athalye, A. (2018). *Evaluating and understanding the robustness of adversarial logit pairing*. arXiv: https://arxiv.org/abs/1807.10272

Evans, D., Calvo, D., Arroyo, A., Manilla, A., & Gómez, D. (2019). End-to-end security assessment framework for connected vehicles. In *22nd International Symposium on Wireless Personal Multimedia Communications (WPMC)* (pp. 1–6). IEEE.

Ferdowsi, A., Ali, S., Saad, W., & Mandayam, N. B. (2019). Cyber-physical security and safety of autonomous connected vehicles: Optimal control meets multi-armed bandit learning. *IEEE Transactions on Communications*, *67*, 7228–7244.

Fernández-Caramès, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, *8*, 21091–21116.

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access*, *7*, 17578–17598.

Fu, Y., Yu, F. R., Li, C., Luan, T. H., & Zhang, Y. (2020). Vehicular blockchain-based collective learning for connected and autonomous vehicles. *IEEE Wireless Communications*, *27*, 197–203.

Gao, J., Obour Agyekum, K. O.-B., Sifah, E. B., Acheampong, K. N., Xia, Q., Du, X., Guizani, M., & Xia, H. (2020). A blockchain-SDN-enabled internet of vehicles environment for fog computing and 5g networks. *IEEE Internet of Things Journal*, *7*, 4278–4291.

Gao, Y., Xu, C., Wang, D., Chen, S., Ranasinghe, D. C., & Nepal, S. (2019). STRIP: A defence against trojan attacks on deep neural networks. In *Proceedings of the 35th Annual Computer Security Applications Conference* (pp. 113–125). ACM.

Garakani, H. G., Moshiri, B., & Safavi-Naeini, S. (2018). Cyber security challenges in autonomous vehicle: Their impact on RF sensor and wireless technologies. In *18th International Symposium on Antenna Technology and Applied Electromagnetics (ANTEM)* (pp. 1–3). IEEE.

Gautham, P. S., & Shanmughasundaram, R. (2017). Detection and isolation of black hole in VANET. In *International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (pp. 1534–1539). IEEE.

Gómez Mármol, F., & Martínez Pérez, G. (2012). Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. *Journal of Network and Computer Applications*, *35*, 934–941. (Special Issue on Trusted Computing and Communications). https://www.sciencedirect.com/science/article/pii/S1084804511000828

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). *Explaining and harnessing adversarial examples*. arXiv: https://arxiv.org/abs/1412.6572

Groza, B., & Murvay, P.-S. (2018). Security solutions for the controller area network: Bringing authentication to in-vehicle networks. *IEEE Vehicular Technology Magazine*, *13*, 40–47.

Gu, S., & Rigazio, L. (2014). *Towards deep neural network architectures robust to adversarial examples*. arXiv: https://arxiv.org/abs/1412.5068

Gu, S., Yi, P., Zhu, T., Yao, Y., & Wang, W. (2019). *Detecting adversarial examples in deep neural networks using normalizing filters*. UMBC Student Collection.

Gu, Z., Han, G., Zeng, H., & Zhao, Q. (2016). Security-aware mapping and scheduling with hardware co-processors for FlexRay-based distributed embedded systems. *IEEE Transactions on Parallel and Distributed Systems*, *27*, 3044–3057.

Guan, Z., Chen, Y., Lei, P., Li, D., & Zhao, Y. (2019). Application of hash function on FMCW based millimeter-wave radar against DRFM jamming. *IEEE Access*, *7*, 92285–92295.

Gudadhe, M., Prasad, P., & Kapil Wankhade, L. (2010). A new data mining based network intrusion detection model. In *International Conference on Computer and Communication Technology (ICCCT)* (pp. 731–735). IEEE.

Guette, G., & Bryce, C. (2008). Using TPMS to secure vehicular ad-hoc networks (VANETs). In J. A. Onieva, D. Sauveron, S. Chaumette, D. Gollmann, & K. Markantonakis (Eds.), *Information security theory and practices. Smart devices, convergence and next generation networks* (pp. 106–116). Springer Berlin Heidelberg.

Gulrajani, I., Ahmed, F., Arjovsky, M., Dumoulin, V., & Courville, A. (2017). *Improved training of Wasserstein GANs*. ACM.

Guo, C., Rana, M., Cisse, M., & Van Der Maaten, L. (2017). *Countering adversarial images using input transformations*. arXiv: https://arxiv.org/abs/1711.00117

Gupta, M., Benson, J., Patwa, F., & Sandhu, R. (2020). Secure V2V and V2I communication in intelligent transportation using cloudlets. *IEEE Transactions on Services Computing*, *15*, 1.

Gupta, R., Kumari, A., & Tanwar, S. (2021). A taxonomy of blockchain envisioned edge-as-a-connected autonomous vehicles. *Transactions on Emerging Telecommunications Technologies*, *32*, e4009.

Gupta, R., Tanwar, S., Kumar, N., & Tyagi, S. (2020). Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Computers & Electrical Engineering*, *86*, 106717.

Gürel, N. M., Qi, X., Rimanic, L., Zhang, C., & Li, B. (2021). Knowledge enhanced machine learning pipeline against diverse adversarial attacks. In *International Conference on Machine Learning* (pp. 3976–3987). PMLR.

Gurung, S., Lin, D., Squicciarini, A., & Bertino, E. (2013). Information-oriented trustworthiness evaluation in vehicular ad-hoc networks. In J. Lopez, X. Huang, & R. Sandhu (Eds.), *Network and system security* (pp. 94–108). Springer Berlin Heidelberg.

Hafeez, A., Topolovec, K., & Awad, S. (2019). Ecu fingerprinting through parametric signal modeling and artificial neural networks for in-vehicle security against spoofing attacks. In *15th International Computer Engineering Conference (ICENCO)* (pp. 29–38). IEEE.

Haider, Z., & Khalid, S. (2016). Survey on effective GPS spoofing countermeasures. In *Sixth International Conference on Innovative Computing Technology (INTECH)* (pp. 573–577). IEEE.

Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., & Witten, I. H. (2009). The WEKA data mining software: An update. *ACM SIGKDD Explorations Newsletter*, *11*, 10–18.

Hassan, Z., Mehmood, A., Maple, C., Khan, M. A., & Aldegheishem, A. (2020). Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles. *IEEE Access*, *8*, 199618–199628.

He, Q., Meng, X., Qu, R., & Xi, R. (2020). Machine learning-based detection for cyber security attacks on connected and autonomous vehicles. *Mathematics*, *8*, 1311. https://www.mdpi.com/2227-7390/8/8/1311

He, Y., Huang, K., Zhang, G., Yu, F. R., Chen, J., & Li, J. (2021). Bift: A blockchain-based federated learning system for connected and autonomous vehicles. *IEEE Internet of Things Journal*, *9*, 12311–12322.

Hegde, N., & Manvi, S. (2019). A novel key management protocol for vehicular cloud security. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *17*, 857.

Heng, L., Work, D. B., & Gao, G. X. (2015). GPS signal authentication from cooperative peers. *IEEE Transactions on Intelligent Transportation Systems*, *16*, 1794–1805.

Hinton, G., Vinyals, O., Dean, J. (2015). *Distilling the knowledge in a neural network*. arXiv: https://arxiv.org/abs/1503.02531

Hossain, M. D., Inoue, H., Ochiai, H., Fall, D., & Kadobayashi, Y. (2020). Lstm-based intrusion detection system for in-vehicle can bus communications. *IEEE Access*, *8*, 185489–185502.

Ivanov, I., Maple, C., Watson, T., & Lee, S. (2018). Cyber security standards and issues in V2X communications for internet of vehicles. *Living in the Internet of Things: Cybersecurity of the IoT*, *2018*, 1–6.

Jadhav, S., & Kshirsagar, D. (2018). A survey on security in automotive networks. In *Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (pp. 1–6). IEEE.

Jain, S., Ahuja, N. J., Srikanth, P., Bhadane, K. V., Nagaiah, B., Kumar, A., & Konstantinou, C. (2021). Blockchain and autonomous vehicles: Recent advances and future directions. *IEEE Access*, *9*, 130264–130328.

Jeon, W., Xie, Z., Zemouche, A., & Rajamani, R. (2020). Simultaneous cyber-attack detection and radar sensor health monitoring in connected ACC vehicles. *IEEE Sensors Journal*, *21*, 1.

Jiang, Q., Ni, J., Ma, J., Yang, L., & Shen, X. (2018). Integrated authentication and key agreement framework for vehicular cloud computing. *IEEE Network*, *32*, 28–35.

Jiang, Q., Zhang, N., Ni, J., Ma, J., Ma, X., & Choo, K. K. R. (2020). Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. *IEEE Transactions on Vehicular Technology*, *69*, 9390–9401.

Jiang, W., Li, H., Liu, S., Luo, X., & Lu, R. (2020). Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles. *IEEE Transactions on Vehicular Technology*, *69*, 4439–4449.

Jin, G., Shen, S., Zhang, D., Dai, F., & Zhang, Y. (2019). APE-GAN: Adversarial perturbation elimination with GAN. In *ICASSP 2019—IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 3842–3846). IEEE.

Jo, H. J., Choi, W., Na, S. Y., Woo, S., & Lee, D. H. (2017). Vulnerabilities of android OS-based telematics system. *Wireless Personal Communications*, *92*, 1511–1530.

Kang, J., Xiong, Z., Niyato, D., Zou, Y., Zhang, Y., & Guizani, M. (2020). Reliable federated learning for mobile networks. *IEEE Wireless Communications*, *27*, 72–80.

Kannan, H., Kurakin, A., & Goodfellow, I. (2018). *Adversarial logit pairing*. arXiv: https://arxiv.org/abs/1803.06373

Kapassa, E., Themistocleous, M., Christodoulou, K., & Iosif, E. (2021). Blockchain application in internet of vehicles: Challenges, contributions and current limitations. *Future Internet*, *13*, 313.

Kapoor, P., Vora, A., & Kang, K. (2018). Detecting and mitigating spoofing attack against an automotive radar. In *IEEE 88th Vehicular Technology Conference (VTC—Fall)* (pp. 1–6). IEEE.

Katragadda, S., Darby, P. J., Roche, A., & Gottumukkala, R. (2020). Detecting low-rate replay-based injection attacks on in-vehicle networks. *IEEE Access*, *8*, 54979–54993.

Kelarestaghi, K. B., Foruhandeh, M., Heaslip, K., & Gerdes, R. (2019). *Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures*. arXiv: https://arxiv.org/abs/1903.01541

Kerrache, C. A., Calafate, C. T., Cano, J., Lagraa, N., & Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access*, *4*, 9293–9307.

Khrulkov, V., & Oseledets, I. (2018). Art of singular vectors and universal adversarial perturbations. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 8562–8570). IEEE.

Kim, H., Hong, S., Kim, J., & Ryou, J. (2020). Intelligent application protection mechanism for transportation in V2C environment. *IEEE Access*, *8*, 86777–86787.

Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, *103*, 102150.

Kishikawa, T., Hirano, R., Ujiie, Y., Haga, T., Matsushima, H., Fujimura, K., & Anzai, J. (2019). Vulnerability of FlexRay and countermeasures. *SAE International Journal of Transportation Cybersecurity and Privacy*, *2*, 21–33.

Korkmaz, K. (2017). Producing the location information with the Kalman filter on the GPS data for autonomous vehicles. In *25th Signal Processing and Communications Applications Conference (SIU)* (pp. 1–4). IEEE.

Krishna, A. M., & Tyagi, A. K. (2020). Intrusion detection in intelligent transportation system and its applications using blockchain technology. In *International Conference on Emerging Trends in Information Technology and Engineering (IC-ETITE)* (pp. 1–8). IEEE.

Kumar, P., Kumar, R., Gupta, G. P., & Tripathi, R. (2022). Bdedge: Blockchain and deep-learning for secure edge-envisioned green CAVs. *IEEE Transactions on Green Communications and Networking*, *6*, 1330–1339.

Kumar, R., Wang, Y., Poongodi, T., & Imoize, A. L. (Eds.). (2021). *Secure vehicular communication using blockchain technology*. Springer. https://doi.org/10.1007/978-3-030-74150-1

Kumar, S., Velliangiri, S., Karthikeyan, P., Kumari, S., Kumar, S., & Khan, M. K. (2021). A survey on the blockchain techniques for the internet of vehicles security. *Transactions on Emerging Telecommunications Technologies*, e4317.

Kumar, V., Ahmad, M., Kumari, A., Kumari, S., & Khan, M. (2021). SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing. *International Journal of Communication Systems*, *34*, e4103.

Kurakin, A., Goodfellow, I., & Bengio, S. (2016). *Adversarial machine learning at scale*. arXiv: https://arxiv.org/abs/1611.01236

Kurakin, A., Goodfellow, I., Bengio, S., Dong, Y., Liao, F., Liang, M., Pang, T., Zhu, J., Hu, X., Xie, C., Wang, J. (2018). Adversarial attacks and defences competition. In *The NIPS'17 Competition: Building Intelligent Systems* (pp. 195–231). Springer.

Kurakin, A., Goodfellow, I. J., & Bengio, S. (2018). Adversarial examples in the physical world. In *Artificial intelligence safety and security* (pp. 99–112). Chapman and Hall/CRC.

Lakshmi, P. S., Saxena, M., Koli, S., Joshi, K., Abdullah, K. H., & Gangodkar, D. (2022). Traffic response system based on data mining and internet of things (IoT) for preventing accidents. In *2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 1092–1096). IEEE.

Lecuyer, M., Atlidakis, V., Geambasu, R., Hsu, D., & Jana, S. (2019). Certified robustness to adversarial examples with differential privacy. In *IEEE Symposium on Security and Privacy (SP)* (pp. 656–672). IEEE.

Leon Calvo, J. A., & Mathar, R. (2018). Secure blockchain-based communication scheme for connected vehicles. In *European Conference on Networks and Communications (EuCNC)* (pp. 347–351). IEEE.

Li, K., Lu, L., Ni, W., Tovar, E., & Guizani, M. (2019). Secret key agreement for data dissemination in vehicular platoons. *IEEE Transactions on Vehicular Technology*, *68*, 9060–9073.

Li, M., Weng, J., Yang, A., Liu, J., & Lin, X. (2019). Toward blockchain-based fair and anonymous AD dissemination in vehicular networks. *IEEE Transactions on Vehicular Technology*, *68*, 11248–11259.

Li, Y., Hou, R., Lui, K.-S., & Li, H. (2018). An MEC-based dos attack detection mechanism for C-V2X networks. In *IEEE Global Communications Conference (GLOBECOM)* (pp. 1–6). IEEE.

Liao, F., Liang, M., Dong, Y., Pang, T., Hu, X., & Zhu, J. (2018). Defense against adversarial attacks using high-level representation guided denoiser. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 1778–1787). IEEE.

Lin, K.-P., Chang, Y.-W., Wei, Z.-H., Shen, C.-Y., & Chang, M.-Y. (2019). A smart contract-based mobile ticketing system with multi-signature and blockchain. In *IEEE 8th Global Conference on Consumer Electronics (GCCE)* (pp. 231–232). IEEE.

Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network*, *31*, 50–58.

Liu, X., Cheng, M., Zhang, H., & Hsieh, C.-J. (2018). Towards robust neural networks via random self-ensemble. In *Proceedings of the European Conference on Computer Vision (ECCV)* (pp. 369–385). Springer.

Liu, X., Yang, H., Liu, Z., Song, L., Chen, Y., & Li, H. H. (2019). DPATCH: An adversarial patch attack on object detectors. *Computer Vision and Pattern Recognition*. https://arxiv.org/abs/1806.02299

Liu, Y., Chen, X., Liu, C., & Song, D. X. (2017). *Delving into transferable adversarial examples and black-box attacks*. arXiv: https://arxiv.org/abs/abs/1611.02770

Liu, Y., Ma, S., Aafer, Y., Lee, W.-C., Zhai, J., Wang, W., & Zhang, X. (2017). *Trojaning attack on neural networks*. Purdue e-Pubs.

Lokesh, B. S., & Kaulgud, N. (2023). A review on analysis of transport layer security in open quantum safe cryptographic algorithm. In *International Conference on Recent Trends in Electronics and Communication (ICRTEC)* (pp. 1–5). IEEE.

Lyamin, N., Kleyko, D., Delooz, Q., & Vinel, A. (2019). Real-time jamming dos detection in safety-critical V2V C-ITS using data mining. *IEEE Communications Letters*, *23*, 442–445.

Lyamin, N., Vinel, A., Jonsson, M., & Loo, J. (2014). Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks. *IEEE Communications Letters*, *18*, 110–113.

Masood, A., Lakew, D. S., & Cho, S. (2020). Security and privacy challenges in connected vehicular cloud computing. *IEEE Communications Surveys Tutorials*, *22*, 2725–2764.

McMahan, B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2017). Communication-efficient learning of deep networks from decentralized data. In A. Singh & J. Zhu (Eds.), *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Vol. 54 of Proceedings of Machine Learning Research* (pp. 1273–1282). PMLR. https://proceedings.mlr.press/v54/mcmahan17a.html

Mendiboure, L., Chalouf, M. A., & Krief, F. (2020). Survey on blockchain-based applications in internet of vehicles. *Computers and Electrical Engineering*, *84*, 106646.

Milaat, F. A., & Liu, H. (2018). Decentralized detection of GPS spoofing in vehicular ad hoc networks. *IEEE Communications Letters*, *22*, 1256–1259.

Mirza, M., & Osindero, S. (2014). *Conditional generative adversarial nets*. arXiv: https://arxiv.org/abs/abs/1411.1784

Mishra, R., Singh, A., & Kumar, R. (2016). Vanet security: Issues, challenges and solutions. In *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 1050–1055). IEEE.

Modas, A., Sanchez-Matilla, R., Frossard, P., & Cavallaro, A. (2020). Toward robust sensing for autonomous vehicles: An adversarial perspective. *IEEE Signal Processing Magazine*, *37*, 14–23.

Möller, D. P. F., Jehle, I. A., & Haas, R. E. (2018). Challenges for vehicular cybersecurity. In *IEEE International Conference on Electro/Information Technology (EIT)* (pp. 0428–0433). IEEE.

Moosavi-Dezfooli, S.-M., Fawzi, A., Fawzi, O., & Frossard, P. (2017). Universal adversarial perturbations. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 86–94). IEEE.

Moosavi-Dezfooli, S.-M., Fawzi, A., & Frossard, P. (2016). *Deepfool: A simple and accurate method to fool deep neural networks*. IEEE.

Moosavi-Dezfooli, S.-M., Shrivastava, A., & Tuzel, O. (2018). *Divide, denoise, and defend against adversarial attacks*. arXiv: https://arxiv.org/abs/abs/1802.06806

Mopuri, K. R., Ojha, U., Garg, U., & Babu, R. V. (2018). NAG: Network for adversary generation. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 742–751). IEEE.

Mousa, A. R., NourElDeen, P., Azer, M., & Allam, M. (2016). Lightweight authentication protocol deployment over FlexRay. In *Proceedings of the 10th International Conference on Informatics and Systems, INFOS'16* (pp. 233–239). Association for Computing Machinery.

Mousavinejad, E., Yang, F., Han, Q.-L., Ge, X., & Vlacic, L. (2020). Distributed cyber attacks detection and recovery mechanism for vehicle platooning. *IEEE Transactions on Intelligent Transportation Systems*, *21*, 3821–3834.

Naresh, V. S., & Thamarai, M. (2023). Privacy-preserving data mining and machine learning in healthcare: Applications, challenges, and solutions. *WIREs Data Mining and Knowledge Discovery*, *13*, e1490. https://doi.org/10.1002/widm.1490

Nguyen, A. M., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 427–436). IEEE.

Nilsson, D. K., & Larson, U. E. (2008). Secure firmware updates over the air in intelligent vehicles. In *ICC Workshops—IEEE International Conference on Communications Workshops* (pp. 380–384). IEEE.

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, *46*, 46–53.

Odena, A., Olah, C., & Shlens, J. (2017). Conditional image synthesis with auxiliary classifier GANs. In *International Conference on Machine Learning* (pp. 2642–2651). PMLR.

Olowononi, F. O., Rawat, D. B., & Liu, C. (2021). Federated learning with differential privacy for resilient vehicular cyber physical systems. In *IEEE 18th Annual Consumer Communications Networking Conference (CCNC)* (pp. 1–5). IEEE.

Otoum, S., Al Ridhawi, I., & Mouftah, H. T. (2020). Blockchain-supported federated learning for trustworthy vehicular networks. In *GLOBECOM 2020—IEEE Global Communications Conference* (pp. 1–6). IEEE.

Pang, T., Xu, K., Du, C., Chen, N., & Zhu, J. (2019). Improving adversarial robustness via promoting ensemble diversity. In *International Conference on Machine Learning* (pp. 4970–4979). PMLR.

Papernot, N., & Mcdaniel, P. (2017). *Extending defensive distillation*. arXiv: https://arxiv.org/abs/1705.05264

Papernot, N., & McDaniel, P. (2018). *Deep k-nearest neighbors: Towards confident, interpretable and robust deep learning*. arXiv: https://arxiv.org/abs/1803.04765

Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z. B., & Swami, A. (2016) *The limitations of deep learning in adversarial settings*. IEEE European symposium on security and privacy (EuroS&P)

Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). Distillation as a defense to adversarial perturbations against deep neural networks. In *IEEE Symposium on Security and Privacy (SP)* (pp. 582–597). IEEE.

Park, J., Lee, S., Oh, C., & Choe, B. (2021). A data mining approach to deriving safety policy implications for taxi drivers. *Journal of Safety Research*, *76*, 238–247. https://www.sciencedirect.com/science/article/pii/S0022437520301675

Park, S., & Park, H. (2022). PIER: Cyber-resilient risk assessment model for connected and autonomous vehicles. *Wireless Networks*, 1–15.

Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In X. Xie, M. W. Jones, & G. K. L. Tam (Eds.), *Proceedings of the British Machine Vision Conference (BMVC)* (pp. 41.1–41.12). BMVA Press.

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, *18*, 2898–2915.

Petit, J., & Shladover, S. E. (2014). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *16*, 546–556.

Petrillo, A., Pescapé, A., & Santini, S. (2020). A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. *IEEE Transactions on Cybernetics*, *51*(3), 1–16.

Pham, M., & Xiong, K. (2020). *A survey on security attacks and defense techniques for connected and autonomous vehicles*. arXiv: https://arxiv.org/abs/2007.08041

Pramanik, M. I., Lau, R. Y. K., Hossain, M. S., Rahoman, M. M., Debnath, S. K., Rashed, M. G., & Uddin, M. Z. (2021). Privacy preserving big data analytics: A critical analysis of state-of-the-art. *WIREs Data Mining and Knowledge Discovery*, *11*, e1387. https://doi.org/10.1002/widm.1387

Qayyum, A., Usama, M., Qadir, J., & Al-Fuqaha, A. (2020). Securing connected autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Communications Surveys Tutorials*, *22*, 998–1026.

Radford, A., Metz, L., & Chintala, S. (2015). *Unsupervised representation learning with deep convolutional generative adversarial networks*. arXiv: https://arxiv.org/abs/1511.06434

Raghunathan, A., Steinhardt, J., & Liang, P. (2020). *Certified defenses against adversarial examples*. arXiv: https://arxiv.org/abs/1801.09344

Rangesh, A., & Trivedi, M. M. (2019). No blind spots: Full-surround multi-object tracking for autonomous vehicles using cameras and lidars. *IEEE Transactions on Intelligent Vehicles*, *4*, 588–599.

Rathee, G., Ahmad, F., Kurugollu, F., Azad, M. A., Iqbal, R., & Imran, M. (2020). CRT-BIOV: A cognitive radio technique for blockchain-enabled internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *22*(7), 1–11.

Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., & Kumar, R. (2019). A blockchain framework for securing connected and autonomous vehicles. *Sensors*, *19*, 3165.

Raya, M., Papadimitratos, P., Gligor, V. D., & Hubaux, J.-P. (2008). On data-centric trust establishment in ephemeral ad hoc networks. In *IEEE INFOCOM 2008—The 27th Conference on Computer Communications* (pp. 1238–1246). IEEE.

Ren, K., Wang, Q., Wang, C., Qin, Z., & Lin, X. (2020). The security of autonomous driving: Threats, defenses, and future directions. *Proceedings of the IEEE*, *108*, 357–372.

Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial attacks and defenses in deep learning. *Engineering*, *6*, 346–360.

Rezgui, J., & Cherkaoui, S. (2011). Detecting faulty and malicious vehicles using rule-based communications data mining. In *IEEE 36th Conference on Local Computer Networks* (pp. 827–834). IEEE.

Rosell, J., & Englund, C. (2021). A frequency-based data mining approach to enhance in-vehicle network intrusion detection. In *Fast zero 21, Society of Automotive Engineers of Japan*. Society of Automotive Engineers.

Rozsa, A., Rudd, E. M., & Boult, T. E. (2016). Adversarial diversity and hard positive generation. *IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 410–417. IEEE.

Sadeghi, K., Banerjee, A., & Gupta, S. K. S. (2020). A system-driven taxonomy of attacks and defenses in adversarial machine learning. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*, 450–467.

Salek, M. S., Khan, S. M., Rahman, M., Deng, H.-W., Islam, M., Khan, Z., Chowdhury, M., & Shue, M. (2022). A review on cybersecurity of cloud computing for supporting connected vehicle applications. *IEEE Internet of Things Journal*, *9*, 8250–8268.

Samangouei, P., Kabkab, M., & Chellappa, R. (2018). *Defense-GAN: Protecting classifiers against adversarial attacks using generative models*. arXiv: https://arxiv.org/abs/1805.06605

Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. *Journal of Big Data*, *7*, 41.

Sedjelmaci, S., Brahmi, I. H., Ansari, N., & Rehmani, M. H. (2018). Cyber security framework for vehicular network based on a hierarchical game. *IEEE Transactions on Emerging Topics in Computing*, *9*(1), 1.

Shao, J., & Wei, G. (2018). Secure outsourced computation in connected vehicular cloud computing. *IEEE Network*, *32*, 36–41.

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS'16* (pp. 1528–1540). Association for Computing Machinery. https://doi.org/10.1145/2976749.2978392

Sharma, A. K., & Mittal, S. K. (2019). Cryptography network security hash function applications, attacks and advances: A review. In *Third International Conference on Inventive Systems and Control (ICISC)* (pp. 177–188). IEEE.

Sharma, P., Austin, D., & Liu, H. (2019). Attacks on machine learning: Adversarial examples in connected and autonomous vehicles. In *IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1–7). IEEE.

Sheik, A. T., & Maple, C. (2019). Key security challenges for cloud-assisted connected and autonomous vehicles. In *Living in the Internet of Things (IoT 2019)* (pp. 1–9). IEEE.

Sheikh, M. S., Liang, J., Wang, W., & Guerrieri, A. (2020). Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wireless Communications and Mobile Computing*. *2020*.

Shoukry, Y., Martin, P., Yona, Y., Diggavi, S., & Srivastava, M. (2015). PYCRA: Physical challenge-response authentication for active sensors under spoofing attacks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS'15* (pp. 1004–1015). Association for Computing Machinery.

Singh, M., & Kim, S. (2018). Trust bit: Reward-based intelligent vehicle commination using blockchain paper. In *IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 62–67). IEEE.

Soll, M., Hinz, T., Magg, S., & Wermter, S. (2019). Evaluating defensive distillation for defending text processing neural networks against adversarial examples. In I. V. Tetko, V. Kůrková, P. Karpov, & F. Theis (Eds.), *Artificial neural networks and machine learning—ICANN 2019: Image processing* (pp. 685–696). Springer International Publishing.

Sommer, F., Dürrwang, J., & Kriesten, R. (2019). Survey and classification of automotive security attacks. *Information*, *10*(4), 148.

Souli, N., Laoudias, C., Kolios, P., Vitale, C., Ellinas, G., Lalos, A., Casademont, J., Khodashenas, P. S., & Kapsalas, P. (2020). GNSs location verification in connected and autonomous vehicles using in-vehicle multimodal sensor data fusion. In *22nd International Conference on Transparent Optical Networks (ICTON)* (pp. 1–4). IEEE.

Srisakaokul, S., Zhang, Y., Zhong, Z., Yang, W., Xie, T., & Li, B. (2018). *MULDEF: Multi-model-based defense against adversarial examples for neural networks*. arXiv: https://arxiv.org/abs/1809.00065

Straub, J., McMillan, J., Yaniero, B., Schumacher, M., Almosalami, A., Boatey, K., & Hartman, J. (2017). Cybersecurity considerations for an interconnected self-driving car system of systems. In *12th System of Systems Engineering Conference (SoSE)* (pp. 1–6). IEEE.

Sun, G., Song, L., Yu, H., Chang, V., Du, X., & Guizani, M. (2019). V2v routing in a VANET based on the autoregressive integrated moving average model. *IEEE Transactions on Vehicular Technology*, *68*, 908–922.

Sun, J., Jin, H., Chen, H., Han, Z., & Zou, D. (2003). A data mining based intrusion detection model. In J. Liu, Y.-M. Cheung, & H. Yin (Eds.), *Intelligent data engineering and automated learning* (pp. 677–684). Springer Berlin Heidelberg.

Sun, X., Yu, F. R., & Zhang, P. (2021). A survey on cyber-security of connected and autonomous vehicles (CAVs). *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 1–20.

Sun, Z., Balakrishnan, S., Su, L., Bhuyan, A., Wang, P., & Qiao, C. (2021). Who is in control? Practical physical layer attack and defense for mmwave-based sensing in autonomous vehicles. *IEEE Transactions on Information Forensics and Security*, *16*, 3199–3214.

Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., & Fergus, R. (2013). *Intriguing properties of neural networks*. arXiv:1312.6199

Tabacof, P., & Valle, E. (2016). *Exploring the space of adversarial images*. IEEE.

Taiyaba, M., Akbar, M. A., Qureshi, B., Shafiq, M., Hamza, M., & Riaz, T. (2020). Secure V2X environment using blockchain technology. In *Proceedings of the Evaluation and Assessment in Software Engineering, EASE'20* (pp. 469–474). Association for Computing Machinery. https://doi.org/10.1145/3383219.3383287

Takahashi, J., Aragane, Y., Miyazawa, T., Fuji, H., Yamashita, H., Hayakawa, K., Ukai, S., & Hayakawa, H. (2017). Automotive attacks and countermeasures on LIN-BUS. *Journal of Information Processing*, *25*, 220–228.

Tangade, S., Manvi, S. S., & Lorenz, P. (2020). Trust management scheme based on hybrid cryptography for secure communications in VANETs. *IEEE Transactions on Vehicular Technology*, *69*, 5232–5243.

Tashiro, A., Muraoka, H., Araki, S., Kakizaki, K., & Uehara, S. (2017). A secure protocol consisting of two different security-level message authentications over can. In *3rd IEEE International Conference on Computer and Communications (ICCC)* (pp. 1520–1524). IEEE.

Tolba, A., & Altameem, A. (2019). A three-tier architecture for securing IoV communications using vehicular dependencies. *IEEE Access*, *7*, 61331–61341.

Trotter, L., Harding, M., Mikusz, M., & Davies, N. (2018). IoT-enabled highway maintenance: Understanding emerging cybersecurity threats. *IEEE Pervasive Computing*, *17*, 23–34.

Valasek, C., & Miller, C. (2014). *Adventures in automotive networks and control units* (Technical White Paper). IOActive.

Van Wyk, F., Wang, Y., Khojandi, A., & Masoud, N. (2019). Real-time sensor anomaly detection and identification in automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *21*, 1264–1276.

Verma, S., Mallick, B., & Verma, P. (2015). Impact of gray hole attack in VANET. In *1st International Conference on Next Generation Computing Technologies (NGCT)* (pp. 127–130). IEEE.

Vitale, C., Piperigkos, N., Laoudias, C., Ellinas, G., Casademont, J., Sayyad Khodashenas, P., Kloukiniotis, A., Lalos, A. S., Moustakas, K., Barrientos Lobato, P., Moreno Castillo, J., Kapsalas, P., & Hofmann, K.-P. (2020). The caramel project: A secure architecture for connected and autonomous vehicles. In *European Conference on Networks and Communications (EuCNC)* (pp. 133–138). IEEE.

Wan, J., Li, J., Imran, M., Li, D., & E Amin, F. (2019). A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics*, *15*, 3652–3660.

Wang, B., Yao, Y., Shan, S., Li, H., Viswanath, B., Zheng, H., & Zhao, B. Y. (2019). Neural cleanse: Identifying and mitigating backdoor attacks in neural networks. In *IEEE Symposium on Security and Privacy (SP)* (pp. 707–723). IEEE.

Wang, D., Li, C., Wen, S., Nepal, S., & Xiang, Y. (2022). Defending against adversarial attack towards deep neural networks via collaborative multi-task training. *IEEE Transactions on Dependable and Secure Computing*, *19*, 953–965.

Wolf, M., Weimerskirch, A., & Paar, C. (2006). Secure in-vehicle communication. In K. Lemke, C. Paar, & M. Wolf (Eds.), *Embedded security in cars* (pp. 95–109). Springer.

Wong, E., & Kolter, Z. (2018). Provable defenses against adversarial examples via the convex outer adversarial polytope. In *International Conference on Machine Learning* (pp. 5286–5295). PMLR.

Wright, P., White, C., Parker, R. C., Pegon, J.-S., Menchetti, M., Pearse, J., Bahrami, A., Moroz, A., Wonfor, A., Penty, R. V., Spiller, T. P., & Lord, A. (2021). 5G network slicing with QKD and quantum-safe security. *Journal of Optical Communications and Networking*, *13*, 33–40.

Wyglinski, A. M., Huang, X., Padir, T., Lai, L., Eisenbarth, T. R., & Venkatasubramanian, K. (2013). Security of autonomous systems employing embedded computing and sensors. *IEEE Micro*, *33*, 80–86.

Xia, L., Sun, Y., Swash, R., Mohjazi, L., Zhang, L., & Imran, M. A. (2022). Smart and secure CAV networks empowered by AI-enabled blockchain: The next frontier for intelligent safe driving assessment. *IEEE Network*, *36*, 197–204.

Xiao, C., Li, B., Zhu, J.-Y., He, W., Liu, M., & Song, D. (2018). *Generating adversarial examples with adversarial networks*. arXiv: https://arxiv.org/abs/1801.02610

Xiao, S., Ge, X., Han, Q.-L., & Zhang, Y. (2021). Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks. *IEEE Transactions on Cybernetics*, *52*(11), 1–13.

Xie, C., Wang, J., Zhang, Z., Zhou, Y., Xie, L., & Yuille, A. L. (2017). *Adversarial examples for semantic segmentation and object detection*. arXiv: https://arxiv.org/abs/1703.08603. IEEE.

Xie, C., Wu, Y., Maaten, L. v. d., Yuille, A. L., & He, K. (2019). Feature denoising for improving adversarial robustness. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 501–509). IEEE.

Xie, G., Yang, L. T., Wu, W., Zeng, K., Xiao, X., & Li, R. (2020). Security enhancement for real-time parallel in-vehicle applications by can FD message authentication. *IEEE Transactions on Intelligent Transportation Systems*, *22*(8), 1–12.

Xiong, W., He, S., & Qiu, T. Z. (2017). Research on connected vehicle architecture based on DSRC technology. In *4th International Conference on Transportation Information and Safety (ICTIS)* (pp. 530–534). IEEE.

Yan, C., Xu, W., & Liu, J. (2016). Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles. *DEFCON*, *24*. 109. https://doi.org/10.5446/36252

Yan, Z., Guo, Y., & Zhang, C. (2018). Deep defense: Training DNNs with improved adversarial robustness. *Advances in Neural Information Processing Systems*, *31*.

Yang, Z., Salman, T., Jain, R., & Pietro, R. D. (2022). Decentralization using quantum blockchain: A theoretical analysis. *IEEE Transactions on Quantum Engineering*, *3*, 1–16.

Yu, Y., Guo, L., Liu, Y., Zheng, J., & Zong, Y. (2018). An efficient SDN-based DDOS attack detection and rapid response platform in vehicular networks. *IEEE Access*, *6*, 44570–44579.

Yuan, X., He, P., Zhu, Q., & Li, X. (2019). Adversarial examples: Attacks and defenses for deep learning. *IEEE Transactions on Neural Networks and Learning Systems*, *30*, 2805–2824.

Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., & Baccelli, E. (2019). Secure firmware updates for constrained IoT devices using open standards: A reality check. *IEEE Access*, *7*, 71907–71920.

Zhang, C., Benz, P., Imtiaz, T., & Kweon, I.-S. (2020). *Understanding adversarial examples from the mutual influence of images and perturbations*. IEEE.

Zhang, D., Shen, Y.-P., Zhou, S.-Q., Dong, X.-W., & Yu, L. (2020). Distributed secure platoon control of connected vehicles subject to dos attack: Theory and application. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*, 1–10.

Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. *Internet of Things Journal, IEEE*, *1*, 10–21.

Zhao, L., Wang, M., Su, S., Liu, T., & Yang, Y. (2020). Dynamic object tracking for self-driving cars using monocular camera and lidar. In *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (pp. 10865–10872). IEEE.

Zheng, S., Song, Y., Leung, T., & Goodfellow, I. (2016). Improving the robustness of deep neural networks via stability training. *Proceedings of the Ieee Conference on Computer Vision and Pattern Recognition*, 4480–4488.

Zheng, T., Chen, C., & Ren, K. (2019). Distributionally adversarial attack. *Proceedings of the AAAI Conference on Artificial Intelligence*, *33*, 2253–2260.

Zheng, Z., & Hong, P. (2018). Robust detection of adversarial attacks by modeling the intrinsic properties of deep neural networks. *Advances in Neural Information Processing Systems*, *31*, 7924–7933.

How to cite this article: Ahmad, J., Zia, M. U., Naqvi, I. H., Chattha, J. N., Butt, F. A., Huang, T., & Xiang, W. (2024). Machine learning and blockchain technologies for cybersecurity in connected vehicles. *WIREs Data Mining and Knowledge Discovery*, *14*(1), e1515. https://doi.org/10.1002/widm.1515