A Comprehensive Survey and Tutorial on Smart Vehicles: Emerging Technologies, Security Issues, and Solutions Using Machine Learning

Usman Ahmad, Mu Han, *Member, IEEE*, Alireza Jolfaei, *Senior Member, IEEE*, Sohail Jabbar, Muhammad Ibrar, Aiman Erbad, *Senior Member, IEEE*, Houbing Herbert Song, *Fellow, IEEE*, and Yazeed Alkhrijah, *Member, IEEE*

***Abstract*— According to research, the vast majority of road accidents (90%) are the result of human error, with only a small percentage (2%) being caused by malfunctions in the vehicle. Smart vehicles have gained significant attention as potential solutions to address such issues. In the future of transportation, travel comfort and road safety will be ensured while also offering several value-added services. The automotive industry has undergone a significant transformation through the use of emerging technologies and wireless communication channels, resulting in vehicles becoming more interconnected, intelligent, and safe. However, these technologies and communication systems are susceptible to numerous security attacks. The objective of this paper is to present a comprehensive overview of the smart vehicle's architecture, encompassing emerging technologies and security challenges and solutions associated with smart vehicles. There has been a significant surge in the utilization of machine learning techniques in smart vehicles. We categorically discuss common security measures, including machine learning and deep learning based solutions that have been mentioned in the literature and implemented against security threats on smart vehicles. This paper has also been titled a tutorial due to its layout, which begins with covering preliminary knowledge, terminologies, and encompassing technologies required to comprehend smart vehicles. Following this, the paper addresses the overall challenges associated with smart vehicles and then focuses on security issues. In terms of solutions, the paper discusses overall solutions to security issues in smart vehicles before delving into a specific solution based on machine learning and deep learning.**

***Index Terms*— Smart vehicles, connected and autonomous vehicles, cybersecurity, security attacks, defence systems, artificial intelligence, machine learning, deep learning, artificial neural networks.**

Manuscript received 16 September 2023; revised 2 January 2024; accepted 12 June 2024. Date of publication 10 July 2024; date of current version 1 November 2024. This work was supported by NPRP through the Qatar National Research Fund (a member of Qatar Foundation) under Grant NPRP13S-0128-200187. The Associate Editor for this article was A. Bucchiarone. *(Corresponding author: Mu Han.)*

Usman Ahmad is with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212003, China, and also with the Department of Computational Sciences, The University of Faisalabad, Faisalabad 38000, Pakistan.

Mu Han is with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212003, China (e-mail: hanmu@ujs.edu.cn).

Alireza Jolfaei is with the College of Science and Engineering, Flinders University, Adelaide, SA 5000, Australia.

Sohail Jabbar is with the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 13318, Saudi Arabia.

Muhammad Ibrar is with the College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar.

Aiman Erbad is with the College of Engineering, Qatar University, Doha, Qatar.

Houbing Herbert Song is with the Department of Information Systems, University of Maryland, Baltimore County (UMBC), Baltimore, MD 21250 USA.

Yazeed Alkhrijah is with the Department of Electrical Engineering, College of Engineering, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh 11564, Saudi Arabia.

Digital Object Identifier 10.1109/TITS.2024.3419988

I. Introduction

AS THE number of vehicles on the road keeps growing, concerns regarding traffic congestion, pollution, and road safety have become increasingly pressing. In the year 2016, there were 37,000 fatalities caused by traffic accidents in the United States [144], while in the European Union [46], the number of fatalities was recorded as 25,500. In December 2018, the World Health Organization released its Global status report on road safety for that year, which revealed that the annual amount of fatalities resulting from road traffic accidents has escalated to 1.35 million [151]. Research indicates that 90% of car accidents are caused by human error, while only 2% can be attributed to vehicle malfunctions [188].

The chart in Figure 1 shows the quantification of road accidents is based on the count of individuals who lost their lives as a result, regardless of whether the fatalities occurred immediately or up to 30 days post-accident [149].

In an effort to address these challenges, smart vehicles have garnered significant attention as potential solutions [64], [137]. A smart vehicle is an umbrella term for a vehicle equipped with cutting-edge technologies. Since the late 1960s [192], microprocessors have been progressively incorporated into automotive engines across the entire engine and drivetrain to enhance overall comfort, braking, and stability. Vehicles of today can include up to one hundred microprocessors. Smart vehicles are an essential element of Intelligent Transportation Systems (ITS) in which vehicles communicate with infrastructure and with other vehicles to exchange critical information and messages (e.g., real-time traffic, road updates, and emergency messages [7]).

Smart vehicles can form ad hoc networks relying on short-range wireless communication technologies such as Wi-Fi to exchange information, called Vehicular Ad hoc Networks (VANETs). Vehicles move speedily and can enter

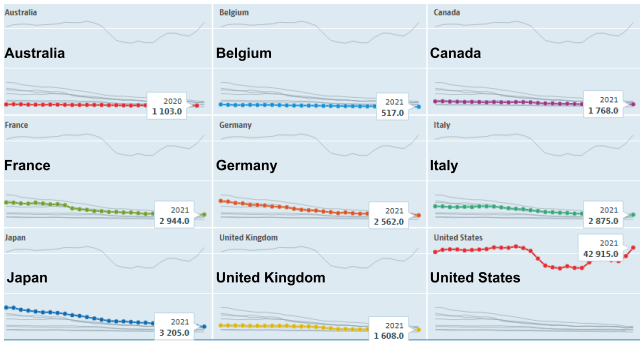

Fig. 1. The count of individuals who lost their lives due to road accidents [149].

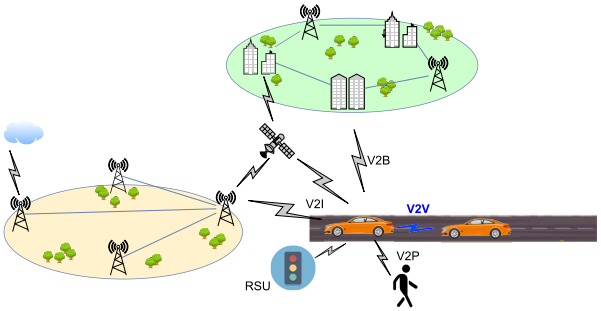

Fig. 2. Some of the specific types of vehicle communication.

and exit the network at any time, which can cause instabilities in signal strength and network topology. So, VANETs require self-organizing and self-configuring capabilities along with robust security measures to protect vehicles against unauthorized access and malicious attacks. The Internet of Vehicles (IoV) terminology refers to the integration of vehicles with the Internet and allows vehicles to exchange information over the Internet. IoV enables new applications and services, such as remote vehicle monitoring and maintenance and on-demand ride-sharing. Moreover, Vehicle-to-Everything (V2X) is a term that refers to the communication between a vehicle and any entity in the surrounding environment. Some of the specific types of communication are Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Device (V2D), Vehicle-to-Pedestrian (V2P), Vehicle-to-Grid (V2G), and Vehicle-to-Building (V2B) communication, as shown in Figure 2.

Autonomous (self-driving) capabilities enable smart vehicles to drive by themselves, using innovative technologies to navigate complex environments. Connected and Autonomous Vehicles (CAVs) use sensors, cameras, and connectivity features for data collection, and utilize this data by using artificial intelligence to make decisions at different levels about how to operate. Sensors and cameras provide real-time information about the road and traffic and can assist autonomous vehicles with tasks like steering, braking, and accelerating. Smart vehicles equipped with Advanced Driver Assistance Systems (ADAS) include features like lane keeping, adaptive cruise control, and collision avoidance. ADAS can enable different degrees of autonomous driving, depending on the features installed in the vehicle.

A. Contribution and Organization of the Paper

This paper presents a comprehensive survey and tutorial on smart vehicles: encompassing emerging technologies, security issues, and the implementation of Machine Learning (ML) and Deep Learning (DL) solutions. Firstly, we have explored the basic building blocks of smart vehicles including Electronic Control Units (ECUs), In-Vehicle Networks (IVNs), including their interconnectivity. Additionally, we explored the various physical interfaces and wireless communication channels utilized in smart vehicles. We also delved into the different kinds of sensors and cameras used in relation to their respective ranges. Secondly, we illustrated the most common emerging technologies in smart vehicles which are transforming the automotive industry. These technologies include the Internet of Things (IoT), Edge Computing, Cloud Computing, Blockchain, and Artificial Intelligence (AI). AI can be employed to address real-world issues by using several techniques. We emphasize the two most common techniques i.e., ML and DL.

The automotive industry is a multifaceted and ever-changing sector that has encountered several challenges and concerns over the years. We distributed these challenges as non-security challenges and security issues. In security issues, we present common attack surfaces and types of security attacks that smart vehicles may face. Finally, we focus on the different methodologies, network technologies, and protocols categorically discussed in the literature and compiled a list of the security measures that have been implemented against the security threats on smart vehicles.

Figure 3 illustrates the arrangement of this paper. Section II delves basic building blocks of smart vehicles such as ECUs, IVNs, sensors, physical interfaces, and wireless communication channels. Emerging technologies in smart vehicles are discussed in Section III. Section IV presents common non-security challenges present in the automotive industry while Section V elaborates on security challenges associated with smart vehicles. Section VI highlights solutions against security attacks including a detailed overview of ML and ANN-based solutions along with information about leading smart vehicle companies. Finally, Section VII concludes the paper. Table I provides a list of the significant acronyms used in this paper.

II. Smart Vehicles

Modern vehicles are characterized as smart vehicles as they have distinct features and are designed with advanced technology, safety, fuel efficiency, and comfort in mind. This section covered the topic of ECUs and IVNs, including their interconnectivity. Additionally, we explored the various physical interfaces and wireless communication channels utilized in smart vehicles. Lastly, we delved into the different kinds of sensors and cameras used in relation to their respective ranges. Figure 4 illustrates the visual representation of this Section.

A. In-Vehicle Architecture

In this segment, the In-Vehicle Architectures are examined, with a focus on ECUs, IVNs, and physical interfaces.

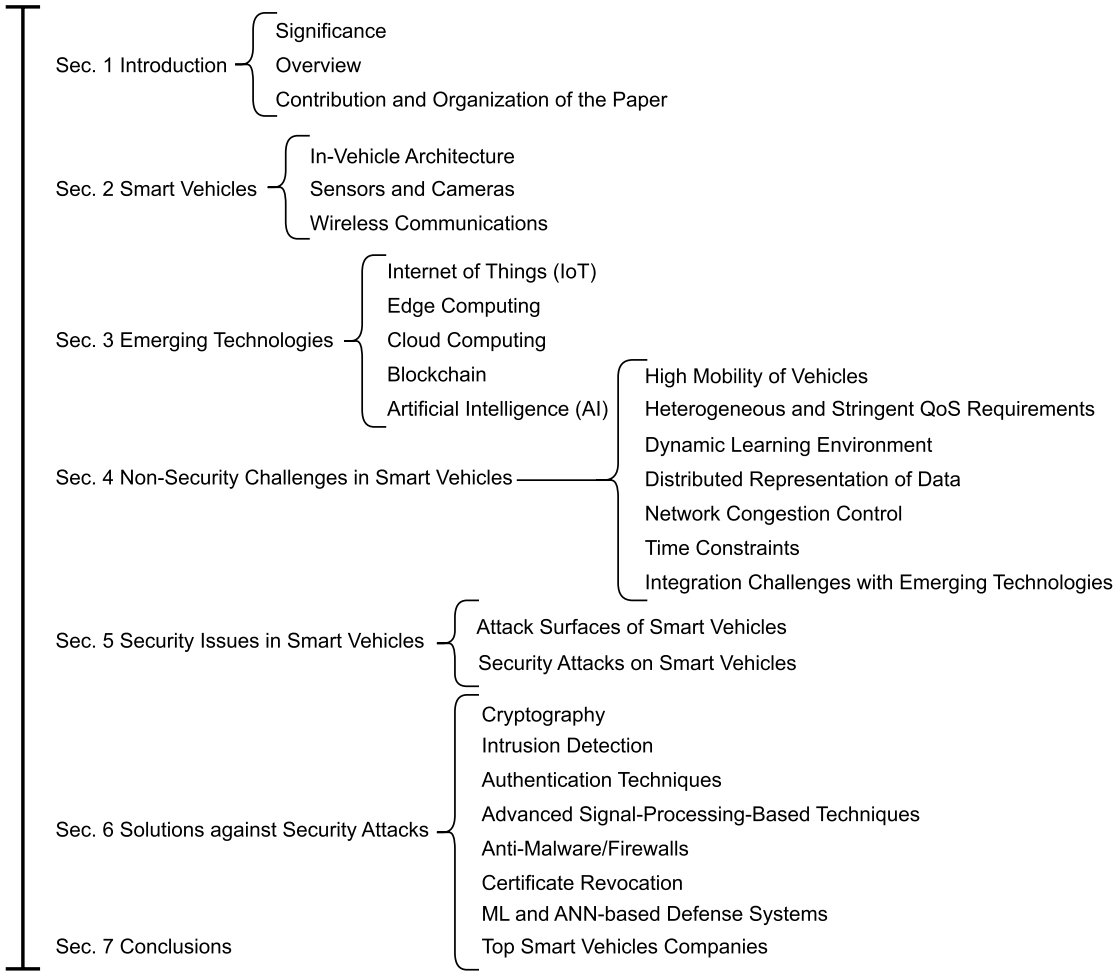

Fig. 3. Outline of the paper.

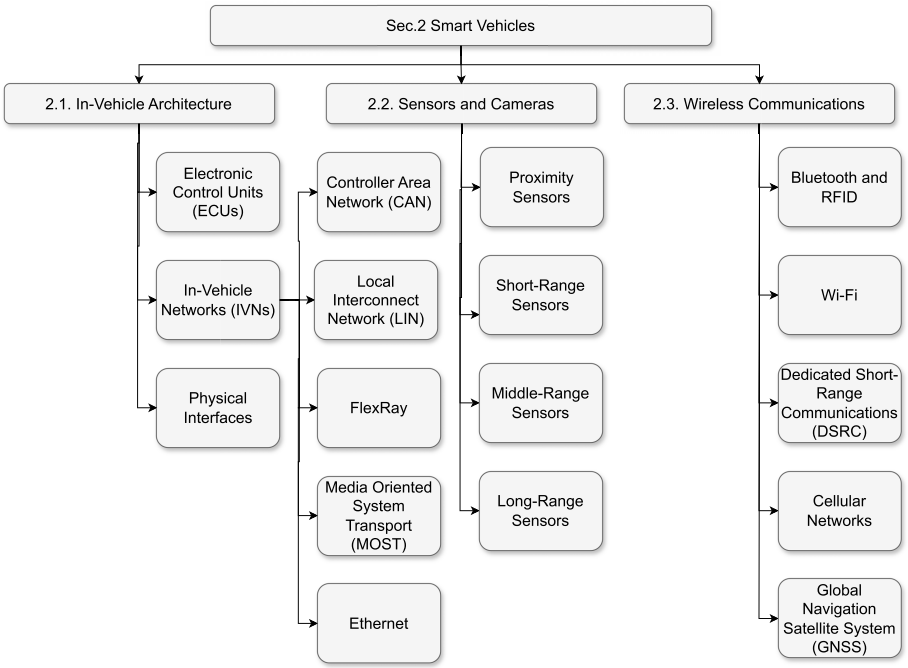

Fig. 4. The visual representation of building blocks of smart vehicles (Section II).

1) Electronic Control Units (ECUs): Smart vehicles typically have numerous interconnected embedded devices called ECUs that control various functions of the vehicle such as engine management, airbag control, and climate control. Most

TABLE I
LIST OF ACRONYMS

ITS	Intelligent Transportation Systems
VANETs	Vehicular Ad hoc Networks
IoV	Internet of Vehicles
V2X	Vehicle-to-Everything
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2P	Vehicle-to-Pedestrian
V2B	Vehicle-to-Building
CAVs	Connected and Autonomous Vehicles
ADAS	Advanced Driver Assistance Systems
ECUs	Electronic Control Units
IVNs	In-Vehicle Networks
IoT	Internet of Things
AI	Artificial Intelligence
CAN	Controller Area Network
LIN	Local Interconnect Network
MOST	Media Oriented System Transport
OBD	On-Board Diagnostics
TPMS	Tire Pressure Monitoring System
OTA	Over-the-air
RFID	Radio Frequency Identification
DSRC	Dedicated Short-Range Communications
GNSS	Global Navigation Satellite System
ML	Machine Learning
DL	Deep Learning
ANN	Artificial Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
GNN	Graph Neural Network
RSUs	Road Side Units

of the vehicles share some basic ECUs, however, the exact number and type of ECUs in a vehicle vary depending on the manufacturer and model. A smart vehicle may contain up to 100 ECUs in addition to basic functions [40]. Some of the common ECUs found in modern vehicles include Engine Control Module, Anti-lock Braking System Control Module, Airbag Control Module, Climate Control Module, Powertrain Control Module, and Lane Departure Warning System [133]. The ECUs communicate with various sensors, actuators, and other ECUs to fetch and interpret data and take decisions accordingly, to regulate the vehicle's systems. The firmware of an ECU is the software written onto the microcontroller that controls the ECU [194]. The manufacturer periodically releases firmware updates to add new features, improve performance, and address bugs.

2) In-Vehicle Networks (IVNs): IVNs are the connectivity standards that provide a means of basic and efficient communication between different ECUs within a vehicle to exchange data and control signals. There are various types of IVNs, each with its own features. As the complexity of vehicles continues to increase, so, IVNs play a significant role in enabling the various ECUs to work together seamlessly. Some of the most common types of IVNs in academia are Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, Media Oriented System Transport (MOST), and Ethernet [88], [196].

- **Controller Area Network (CAN) bus** is a well-known industry standard for in-vehicle communication, developed in the 1980s by the German company Bosch [153]. CAN bus is an event-triggered communication protocol in smart vehicles to connect ECUs to the other ECUs, physical ports, and other IVNs. It is a multi-master serial bus supporting a large number of nodes and transmitting data with up to 1 Mbps data rates [120]. CAN bus allows each ECU in a vehicle to communicate with all other ECUs over a single bus, reducing the amount and cost of cabling and simplifying the overall wiring harness. CAN bus is a two-wire (CAN low and CAN high) communication protocol that facilitates the ECUs to receive and broadcast information. The broadcasted data is accepted by all ECUs on IVN, and each ECU then checks the data and decides whether to receive or ignore it. The functionality of the CAN bus can be unified in the 7-layer OSI model [62]. In the case of a high-speed CAN bus, it is illustrated by a data link layer (ISO 11898-1) and a physical layer (ISO 11898-2). CAN logger is used to take records of CAN messages called frames. CAN ID and data are two important fields of the CAN frame to keep track of timestamped CAN messages to an SD card or to a PC.
- **Local Interconnect Network (LIN) bus** was developed by several automakers, including BMW, Volkswagen, and Volvo, and is intended for the cost-effective replacement of the CAN bus. LIN is a single-wire communication standard with simple and lower data rates. LIN is not as reliable as the CAN buses so used in conjunction with CAN or other IVNs and is particularly used for communication between such ECUs which are not time critical such as climate control, mirrors lift, and lighting [212].
- **FlexRay** was created by BMW in 2007 and is intended for both synchronous and asynchronous data transmission using two parallel channels [180]. FlexRay has a data throughput of up to 10 Mbps per channel, which is quicker than other IVNs like CAN and LIN. It can transmit time-critical messages and event triggers at the same time. Although it provides higher bandwidth and improved reliability, implementing the FlexRay protocol may come with additional costs and often limits its practical deployment [212].
- **Media Oriented System Transport (MOST)** is a high-speed communication standard that specifically used the transmission of audio and video data between different ECUs such as the infotainment system, dashboard display, GPS navigation, and amplifier [180]. MOST technology uses a fiber optic cable which allows for the transfer of large amounts of data at rates up to 150 Mbps [50]. MOST is a high-speed multimedia communication technology, while CAN and LIN are designed for lower-speed real-time control and monitoring. MOST, CAN, and LIN are all used for communication in smart vehicles, but they have different features, costs, complexity, and compatibility issues.
- **Ethernet** is becoming increasingly prevalent and considered a replacement for legacy IVNs due to the growing demand for high-speed data rates within smart vehicles [101], [183]. However, there are also some challenges and issues associated with the adoption of Ethernet in smart vehicles. Some of the main challenges are the need to ensure reliable communication while dealing with harsh environmental conditions and robust security

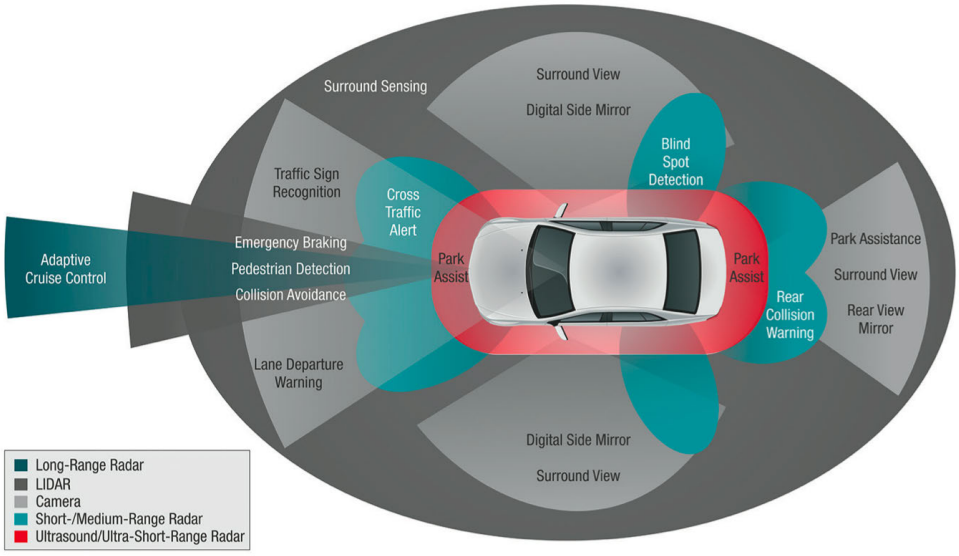

Fig. 5. The primary sensor types utilized by CAVs, along with their range and location (figure taken from [175]).

measures to protect against cyber-attacks associated with the adoption of Ethernet technology.

3) Physical Interfaces: There are several physical interfaces in smart vehicles that allow external devices to connect and communicate with the IVNs and ECUs. These interfaces can be used for a variety of purposes such as diagnostics, programming, data logging, and audio/video data transmission. On-Board Diagnostics (OBD-II) port is a mandatory standard diagnostic interface that is found in smart vehicles [186]. It is typically located under the dashboard and can be used to diagnose and troubleshoot vehicle problems. Aftermarket devices are products that are added to a vehicle after it has been purchased from the original equipment manufacturer. The security of these devices can be uncertain and it is a significant challenge to ensure their security. These devices can be connected through USB ports, auxiliary input jacks, HDMI ports, SD card slots, AC power outlets, etc.

B. Sensors and Cameras

Smart vehicles use numerous sensors to monitor and control various in-vehicle functions. These sensors perceive data from the real-time environment, transfer it to the vehicle's ECUs to process this data, and make decisions as needed to ensure that the vehicle is operating safely and efficiently. Smart vehicles use a variety of sensors; each has a specific purpose and particular type of data collection such as an oxygen sensor, accelerometer, gyroscope, Tire Pressure Monitoring System (TPMS) sensor, fuel level sensor, and so on [160]. Autonomous features in smart vehicles are made possible not only by artificial intelligence but also by adding various special-purpose sensors and cameras. These sensors and cameras collect data about the vehicles and their surroundings, including information about the vehicle itself (e.g., speed, location), roads, obstacles, other vehicles, and pedestrians.

Sensors used in autonomous vehicles can be classified in regard to their sensing range such as proximity (5m), short-range (30m), middle-range (80-160m), and long-range (250m) sensors [160]. Each of these sensors operates within its designated range, but they work in conjunction to perceive the environment. The primary sensor types utilized by CAVs, along with their range and location are shown in Figure 5 [175].

1) Proximity Sensors: The ultrasonic sensor is a proximity sensor used in smart vehicles [197], that emits ultrasound waves that bounce off objects. It is specifically designed to detect nearby objects while the vehicle is moving at a slow speed, particularly serving to assist in parking.

2) Short-Range Sensors: Short-Range Sensors can be classified into two types: (1) forward and backward cameras and (2) Short-Range RADAR (SRR). These Cameras capture images of the environment and can be used for object detection, lane following, and traffic sign recognition. The forward cameras aid in recognizing traffic signs and detecting lane departure, while the backward cameras provide support for parking. RADAR sensors use radio waves to detect objects and measure their distance, speed, and angle of approach [197]. SRR assists in detecting blind spots (which cannot be directly seen by the driver) and alerting drivers to cross-traffic.

3) Middle-Range Sensors: The LIDAR and Medium-Range RADAR (MRR) have a range that falls within the medium category and they are primarily utilized to detect pedestrians and prevent collisions and crashes. LIDAR sensors emit laser pulses and measure the time taken for the reflections to return, creating a map of the vehicle's surroundings [97].

4) Long-Range Sensors: Long-Range RADAR (LRR) makes it possible to implement Adaptive Cruise Control (ACC) even when driving at high speeds [181].

Autonomous capabilities are achieved through the use of various sensors (as discussed above) and cameras, in combination with data collected from V2V, V2I communication, and internal sensors such as speed sensors and GPS.

C. Wireless Communications

Smart vehicles are equipped with advanced wireless communication technologies that allow IVNs to communicate with

external systems and networks both inside and outside the vehicle [30], [74]. Wireless communication technologies in vehicles inherit numerous features such as Over-the-air (OTA) updates and MirrorLink to enhance the efficiency and overall driving experience. OTA updates ability in vehicles allows them to wirelessly update the firmware and software system to deploy software fixes, new features, and security patches without requiring owners to bring them into a service center. MirrorLink is one of the most commonly used technology standards that allow smartphones to be connected to vehicles via Bluetooth, Wi-Fi, or USB. It enables drivers to access and control their smartphones through the vehicle's dashboard display, making it easier and safer to use while driving. Common types of wireless communication equipment used in smart vehicles are given below:

1) Bluetooth and RFID: Bluetooth is a set of specifications that conform to a wireless technology standard and enable communication and data transfer among various types of devices over short distances [52]. It is commonly integrated into infotainment systems in vehicles, primarily for linking mobile devices, tablets, laptops, and headphones. Bluetooth connections frequently include features like audio, and media streaming, web browsing through a cellular network, and relaying of text messages [116].

Radio Frequency Identification (RFID) technology is commonly used in smart vehicles for short-range communication applications such as keyless entry and start systems and tire pressure monitoring systems. Zigbee is a wireless communication standard that is also used in smart vehicles to connect various components and sensors, such as those for climate control, tire pressure monitoring, and collision detection. Radio and infrared connections [42] have been utilized for the purpose of V2V communication.

2) Wi-Fi: Wireless Local Area Networks are networks that use wireless communication to connect multiple devices within a specific area. The most famous implementation of WLANs is Wi-Fi, which is widely used for providing wireless Internet access. Vehicle manufacturers are offering built-in Wi-Fi to provide Internet connectivity and Wi-Fi hotspots as a standard or optional feature in their vehicles [2]. Wi-Fi hotspot allows passengers to connect their handheld devices (e.g., smartphones and laptops) to the vehicle's Wi-Fi network and access the Internet without using their own mobile data plans. In addition to providing Internet connectivity for passengers, Wi-Fi is also being used in smart vehicles for V2V, V2I, and V2X communication. Wi-Fi can also be used to provide over-the-air software updates for vehicle systems and components.

3) Dedicated Short-Range Communications (DSRC): VANETs configuration have been developed over time, such as the use of Dedicated Short-Range Communications (DSRC) in the US and ITS-G5 in Europe used for V2V and V2I communication [179]. DSRC is a variant of Wi-Fi that operates within the top end of the Wi-Fi frequency range. Specifically, Wi-Fi follows the IEEE 802.11 set of standards, while DSRC protocol adheres to the guidelines outlined in the IEEE 802.11p standard. DSRC is a technology that enables V2V and V2I communication over short distances. However, a recent study revealed several challenges related to the short-range, scalability, and infrastructure deployment of the DSRC [16]. There has been a drive toward using cellular networks for V2X communication in order to get around DSRC limitations.

4) Cellular Networks: Cellular networks are a type of wireless network that enable smart vehicles to become more connected to the internet [61]. It has the capability of V2V and V2X communication over significantly long distances due to its much greater range than Wi-Fi and DSRC [92]. The generations of cellular networks are typically referred to as 1G, 2G, 3G, 4G, and 5G. Each generation represents significant improvements in terms of speed and efficiency. 5G connectivity provides faster and more reliable internet access to smart vehicles.

5) Global Navigation Satellite System (GNSS): Smart Vehicles must include the Global Navigation Satellite System (GNSS), which uses a network of satellites to monitor the location and motion of the car in real time. It is made up of a network of satellites that send signals to receivers on the ground so they can determine their exact location and speed. Any global navigation satellite system, including GPS (USA), BeiDou (China), GLONASS (Russia), and Galileo (Europe), is referred to as a GNSS [15]. While GPS is the most well-known GNSS, each system has particular benefits and drawbacks of its own.

III. Emerging Technologies

In this paper, emerging technologies refer to common information and communication technologies and advancements that are recently noticed and are still largely unexplored in terms of their development or practical applications in the automotive industry. These advancements can include both brand-new technologies as well as previously established ones that are now being utilized in novel ways. Some of the most common emerging technologies in smart vehicles are discussed in this section, which are transforming the automotive industry. Table II highlights the major role played by the discussed emerging technologies. Figure 6 shows a graphical depiction of this Section.

A. Internet of Things (IoT)

IoT has revolutionized the automotive industry by making vehicles more connected, intelligent, and safer [102]. IoT in automotive is an intricate network of interconnected devices such as sensors, cameras, and GNSS that are linked to the cloud through the Internet. This network constantly provides real-time data which can be used to improve transport management efficiency.

One of the most notable IoT applications in modern vehicles is CAVs. CAVs use IoT technologies to connect to the internet which allows for navigating roads and safely transporting passengers without human intervention. With the integration of IoT technologies, the vehicle uses sensors, cameras, GNSS, and wireless communication channels to provide real-time data about surroundings, vehicle location, and driver behavior. This information enables self-driving features and can be used to optimize vehicle performance and maintenance, improve fuel efficiency, and enhance driver safety. As technology continues

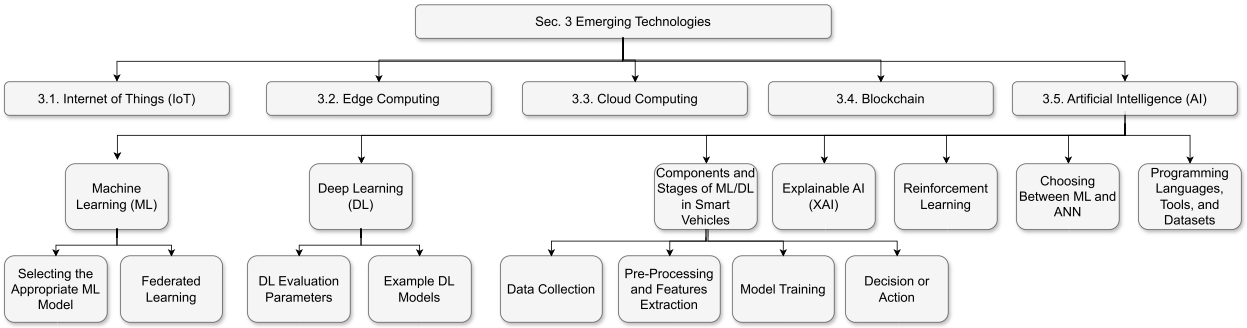

Fig. 6. A graphical depiction of the emerging technologies (Section III).

TABLE II
COMMON EMERGING TECHNOLOGIES IN SMART VEHICLES

Technology	Key Points	Papers
IoT	An intricate network of interconnected devices such as sensors (PKES and TPMS etc.), cameras, and GNSS	[102], [45]
Edge Computing	Allows for data to be processed locally for ensuring quick and accurate decision-making by the vehicle's onboard computer	[121], [168]
Cloud Computing	Offers practically infinite storage space, enabling to store of large amounts of data to deal with enormous quantities of data (e.g., facilitates OTA software updates)	[113], [18], [61], [29]
Blockchain	Provide a decentralized ledger, ensure the authenticity and tamper-proof record of a vehicle	[230], [93], [142]
AI (ML, DL)	ADAS and CAVs mainly rely on AI algorithms to navigate roads, avoid obstacles, make safe driving decisions, predictive maintenance, and so on.	[27], [150], [12], [160], [161], [12], [122], [12], [111], [3]

to evolve, we can expect more innovative IoT applications in smart vehicles in the future. It is projected that the widespread adoption of CAVs in the automotive industry would result in significant economic effects, with an estimated value of $1.2 trillion or $3,800 per American annually [45].

B. Edge Computing

CAVs technology has naturally embraced edge computing as a fundamental component owing to its ability to process data locally in real-time [121]. CAVs generate massive amounts of data from sensors and cameras. Processing this data in real-time is critical for ensuring quick and accurate decision-making by the vehicle's onboard computer. Edge computing allows for this data to be processed locally, which reduces latency and improves overall performance. At present, edge computing artificial intelligence programs are being employed by all CAVs on the road.

Smart vehicles also leverage edge computing for predictive maintenance, which involves analyzing data from multiple sensors and ECUs such as engine temperature, tire pressure, and battery health [168]. By using algorithms at the edge, possible problems can be detected before they escalate and cause breakdowns. This proactive approach to maintenance can not only prevent expensive repairs but also reduce vehicle downtime.

C. Cloud Computing

Cloud computing has been widely used for data backup, software development and testing, disaster recovery, and other purposes. However, recently, the popularity of cloud computing has increased dramatically in the automotive industry [18], [113]. With the emergence of CAVs features, the growth of cloud computing in the automotive industry is remarkable. CAVs rely on sensors, cameras, and GNSS to operate without a human driver. To facilitate the continuous exchange of data between vehicles and their surroundings, automotive cloud solutions provide uninterrupted network services. By leveraging cloud platforms, CAVs can enhance their safety, efficiency, and security.

The automotive sector deals with enormous quantities of data, and storing it requires a significant amount of storage capacity. Traditional on-premises data storage methods necessitate the purchase of costly storage devices. Cloud computing solutions offer practically infinite storage space, enabling you to store large amounts of data. Furthermore, you can easily expand your storage capabilities as your needs evolve. The utilization of the cloud in the automotive industry can effectively lower expenses. Intelligent automotive cloud solutions offer a pay-per-use or subscription approach, allowing you to pay solely for the resources and storage used, with the ability to adjust as per your needs [29], [61].

Cloud technology also facilitates OTA software updates, which add new features and improves vehicle performance without the need for physical visits to the dealership. In addition, cloud integration can enhance in-vehicle entertainment and infotainment systems by enabling the streaming of music, movies, and other media. As a result, cloud computing is becoming an essential technology for smart vehicles.

D. Blockchain

According to Chris Ballinger, who is affiliated with the Toyota Research Institute, the implementation of blockchain

technology can accelerate the arrival of autonomous vehicles on our roads [230]. Blockchain is a distributed digital ledger with a series of records, known as blocks that are linked together using secure cryptographic hashes. It enables transparent information sharing within a business network. Each block includes a timestamp, transaction data, and a cryptographic hash of the previous block. These blocks function as a chain, where each subsequent block links to the ones before it. Altering any given block retroactively would require modifying all subsequent blocks, hence making blockchain transactions irreversible. The decentralized nature of blockchain makes it a secure way to store and transfer data or assets because it is difficult for malicious actors to alter the data once it has been recorded on the blockchain. Blockchain technology has the potential to revolutionize modern vehicles by providing a secure and transparent way to share and track crucial data [93], [142]. The blockchain can be utilized by the automotive sector in numerous ways, as given below:

- In the context of CAVs, there are several critical factors they need to constantly monitor, including road conditions, their own state, and the status of other vehicles. Traditional IoT can make this process complicated due to its communication protocols. However, with the decentralized ledger of blockchain technology, every node in the network (such as each vehicle and data point) can almost instantly and accurately access all the data. There are ongoing efforts to integrate better vehicle tracking and communication to enhance overall connectivity, and developing decentralized networks that transfer data more smoothly to all points is a crucial step toward creating a secure ecosystem for autonomous vehicles.
- Vehicle manufacturers can ensure the authenticity of their spare auto parts and monitor the whereabouts of a specific vehicle along their supply chain. As per Matthew Jones, an IBM representative, automobile companies that leverage blockchain technology to establish the origin of their spare parts can considerably reduce costs associated with recall operations.
- Blockchain can help create a tamper-proof record of a vehicle's history, including its ownership, accident history, and maintenance records. This can be especially useful when insuring, buying, or selling a used car, as it can provide transparency about the vehicle's condition and history.

E. Artificial Intelligence (AI)

The term AI was first adopted by John McCarthy, a retired professor from Stanford University, in 1955 [161]. The original definition of AI referred to a machine's capacity to accomplish tasks that previously demanded human intelligence. However, this description was quite comprehensive and has since undergone various modifications over the course of decades of research and technological progress. A robust AI workflow involves tasks such as data preparation, model creation, system design for model implementation, and deployment on hardware or enterprise systems. The impact of AI has been felt in diverse areas such as education, healthcare, cybersecurity, smart homes, agriculture, energy management, environmental monitoring, supply chain management, legal services, fraud detection, marketing, finance, banking, gaming, and so on.

AI has become an increasingly important component in smart vehicles, some common applications of AI in smart vehicles are discussed in this paragraph. ADAS is a prominent feature of smart vehicles and owes much to AI's pivotal role in its development. ADAS and CAVs rely on AI to navigate roads, avoid obstacles, and make safe driving decisions. In CAVs, complex environments are enabled with automation through the integration of AI algorithms in AI-driven systems. At present, AI programs are being employed by all CAVs on the road. AI-powered predictive maintenance platforms can analyze data from sensors throughout the vehicle to detect potential issues before they become major problems. In addition, some automakers are experimenting with AI to create personalized driving experiences based on a driver's preferences and habits. AI can be employed to address real-world issues by using several techniques, some of the most common techniques are given below:

1) Machine Learning (ML): ML is an AI approach that enables machines to learn from experience. Instead of relying on a pre-determined equation as a model, ML algorithms use computational methods to directly learn information from data. There are two main types of techniques utilized in ML. The first one is supervised learning, which involves training a model on input and output (also called labels) data that is known to predict future outputs (i.e., classification or regression) accurately. The second technique is unsupervised learning, which focuses on discovering hidden patterns or inherent structures within input data (unlabeled data) and splitting this data into clusters. ML relies on multiple dataset types, including text, audio, image, video, time series, and graph datasets that serve the purposes of training, validation, and testing.

a) Selecting the Appropriate ML Model: Identifying the ideal ML method is not straightforward, and there isn't a universal solution that always works. It's often a matter of trial and error, and even expert data scientists cannot ascertain whether a ML algorithm will succeed without putting it into practice. However, selecting the appropriate ML algorithm also hinges on factors such as the volume and nature of the data, the desired outcomes from analyzing the data, and how these insights will be utilized. Some of the popular ML algorithms are linear regression, logistic regression, decision tree, Support Vector Machine (SVM), naive bayes, nearest neighbor, K-means, random forest, and Principal Component Analysis (PCA) [27].

b) Federated Learning: The dataset is typically centralized, but in some cases, it can be distributed across multiple devices or locations [219]. A state-of-the-art ML method called federated learning trains an algorithm through many separate sessions, each utilizing its own dataset. Federated learning, also known as collaborative learning, is a decentralized technique for training ML models that don't involve sending data from client devices to global servers. Rather than that, the raw data available on edge devices is utilized to locally train the model, resulting in enhanced data privacy.

c) Fuzzy Logic: Fuzzy logic, a branch of AI, can also be applied in autonomous vehicles to imitate human decision-making. For example, the authors have proposed a collision avoidance system for smart vehicles, by applying a fuzzy logic scheme to draw inspiration from human social norms [172].

2) Deep Learning (DL): DL is a type of ML technique that is a layered structure of interconnected nodes or neurons that imitates the human brain and is known as an Artificial Neural Network (ANN). The ANN is composed of three layers, namely the input layer, one or more hidden layers, and an output layer. In the context of ANNs, the term "deep" typically signifies the number of hidden layers. Unlike traditional neural networks which usually contain 2-3 hidden layers, deep networks can have an extensive range of 150 hidden layers or more [12]. Each layer contains several neurons which utilize the previous layer's outputs as inputs. This produces a complex interconnected system in which all neurons are linked through various layers. During the learning process, each neuron receives an assigned weight that is constantly adjusted, with decreases or increases in the weight modifying the strength of that neuron's signal. Similar to other ML algorithms, ANNs are applicable for both supervised learning, which comprises classification and regression, as well as unsupervised learning, which deals with pattern recognition and clustering [111].

a) DL Evaluation Parameters: Some of the most common parameters of ANN evaluation include accuracy, precision, recall, F1 score, confusion matrix (true positives, false positives, true negatives, and false negatives), and Receiver Operating Characteristic (ROC) curve. Precision is a metric that evaluates the accuracy by measuring the ratio of true positive predictions to the total number of instances predicted as positive. The recall is another metric that assesses the completeness of a model by measuring the ratio of true positive predictions to the total number of actual positive instances.

b) DL Model Example: The most commonly used ANNs are:

- Convolutional Neural Networks (CNN) are one of the most used ANNs. The two fundamental components of a CNN are feature extraction and classification. They operate by convolving learned features with input data and utilize 2D convolutional layers, making them particularly effective for processing 2D data, such as images. One of the benefits of using CNNs is that they eliminate the necessity for manual feature extraction. Therefore, there is no requirement to manually identify the features that are employed to classify images. CNNs were originally developed for image recognition tasks, but they have also been successfully applied to Natural Language Processing (NLP) tasks. NLP focuses on enabling machines to understand, interpret, and generate human language.
- A type of ANN called Recurrent Neural Network (RNN) is designed to capture sequential dependencies in input data, such as time series, sensor readings, and text. One of the most commonly used RNN architectures is the Long Short-Term Memory (LSTM) network, which utilizes feedback loops to model these dependencies.
- Graphs are ubiquitous, and objects in the real world are frequently defined based on their interconnections with other entities. In essence, a graph denotes the connections (links or edges) that exist between various entities (vertex or nodes) within a group. A Graph Neural Network (GNN) is a type of ANN that operates on graph-structured data. GNN can provide better predictions about entities involved in these interactions by extracting and utilizing features from the underlying graph, unlike models that only consider individual entities in isolation. Practical applications of GNNs are emerging in diverse areas, including traffic prediction [150]. GNNs have many flavors, some of the common embedding computations are Graph Convolutional Networks (GCN), Graph Attention Networks (GAT), Graph Sample and Aggregate (GraphSAGE), and Graph Isomorphism Networks (GIN).

A hybrid approach in ANNs refers to combining two or more different ANN architectures to achieve better performance. In [226], a model for image classification is proposed that is a combination of CNN and RNN called the CNN-RNN model. In [128], the authors demonstrated a hybrid approach based on image processing and speech recognition in IoV to automatically drive the vehicles.

3) Components and Stages of ML/DL in Smart Vehicles: The four main components that can benefit from ML/ANN in the driving task elements of CAVs are perception, prediction, planning, and decision-making and control [160].

- Perception helps with recognizing objects in the surrounding environment
- Prediction forecasts the actions of other objects such as vehicles and pedestrians
- Planning the route of the vehicle to reach its destination
- Making decisions regarding the movement and control of the vehicle

The implementation of ML/ANN in CAVs involves a sequence of stages, which are as follows:

a) Data Collection: Input data is collected either via sensors, cameras, communication channels (physical and wireless), ECUs, IVNs, and or other digital means.

b) Pre-Processing and Features Extraction: The collected data, comprising heterogeneous information such as images, videos, and traffic data (textual data), is digitally processed, and appropriate features are extracted.

c) Model Training: Using the extracted features from input data, an ML/ANN model learns to differentiate various objects and events encountered in the driving environment. For instance, the model can recognize moving objects like pedestrians, vehicles, and cyclists, as well as distinguish between different traffic signs such as stop and speed limit signs.

d) Decision or Action: Based on the knowledge acquired by the vehicular network, a decision or action is executed, such as stopping the vehicle at a stop sign or predicting traffic flow. This is performed according to the learned knowledge and underlying system.

4) Explainable AI (XAI): The complexity of ANNs is so high that it becomes nearly impossible for their inventors and developers to comprehend their internal functions, thus leading

to the term "black box". The goal of Explainable AI (XAI) is to provide responses to inquiries from stakeholders regarding the AI systems' processes for making decisions [216].

5) Reinforcement Learning: Reinforcement learning is a type of ML methodology in which an agent learns how to perform a specific task by repeatedly interacting with a changing environment. By receiving rewards or penalties based on its actions, the agent updates its decision-making strategy and strives to achieve the task's maximum reward without any human intervention or explicit programming. This approach of learning through trial and error allows the agent to make decisions that optimize the given reward metric. The reinforcement learning algorithms like DQN, A2C, and DDPG are used for training policies. Reinforcement learning is a viable option for making driving decisions in CAVs using camera input, mainly due to the remarkable success of deep neural networks in image-based applications.

6) Choosing Between ML and ANN: The results of the experiments demonstrate that DL techniques outperform traditional ML approaches in various fields such as image processing, computer vision, speech recognition, machine translation, art, medical imaging, medical information processing, robotics and control, bio-informatics, Natural Language Processing, cybersecurity, and more. The performance achieved by DL methods is considered state-of-the-art [12].

First of all, if you are dealing with a challenging task or problem that has numerous variables and involves processing a vast amount of data, but lacks an established formula or equation, it is advisable to explore the potential of ML or ANN. Feature extraction is a crucial step in ML/ANN where the input data is carefully chosen and transformed to create a new representation that is better suited for a specific task. In ML, one would typically select features and a classifier manually in order to categorize images. However, with ANN, the processes of feature extraction and modeling are automated. Moreover, ANN applies an "end-to-end learning" method where a network is fed raw data and a specific task to accomplish, such as classification, and it learns how to do this autonomously. For example, PCA is used to reduce the dimensionality of high-dimensional data by projecting it onto a lower-dimensional space; CNNs are particularly well-suited to image-processing tasks. They work by applying a series of convolutional filters to an input image to extract features at various levels of abstraction. Similarly, RNNs are designed to process sequences of inputs.

Secondly, when deciding between ML and ANN, it is important to take into account whether you possess a high-performance GPU as well as an abundance of labeled data. If either of these components is lacking, utilizing ML instead of ANN may prove more advantageous. For an ANN application to be successful, it is necessary to have a substantial amount of data (thousands of images in the case of image dataset) for training the model. Additionally, GPUs are required to swiftly process this data.

In the event that you opt for ML, you possess the ability to train your model with numerous classifiers. You may also already be familiar with which features to extract that will produce optimal results. Moreover, you have the flexibility to experiment with various combinations of approaches, classifiers, and features to determine the most effective arrangement for your data.

7) Programming Languages, Tools, and Datasets for ML and ANN:

- Programming Languages:
  Take a glance at the primary languages that are most in demand and commonly used to implement the ML and ANN algorithms, such as Python, R, C++, Java, JavaScript, Julia, and LISP. There are many libraries used for ML and ANN, as they provide a way to reuse code, optimize performance, standardize common tasks, and extend functionality. By using these libraries, developers can save time and effort by leveraging pre-existing solutions for common problems instead of starting from scratch every time. Some of the most popular ones are Scikit-Learn, Tensorflow, Keras, PyTorch, OpenCV, Theano, Caffe, and so on.
- ML/DL Tools: There are some cloud-based ML platforms enable programmers to write and execute code directly in their web browser without requiring any setup or configuration. For example, colaboratory (also known as "Colab") is a tool developed by Google Research that enables individuals to write and run Python code directly in their web browser. Its capabilities make it particularly advantageous for ML tasks. Similarly, Amazon SageMaker is another cloud-based ML platform that was introduced in 2017. It can be accessed without requiring any setup on the user's end.
- Simulation Tools: According to Liu et al. [122], the leading platform for autonomous driving currently is the NVIDIA Drive PX2 [54]. This platform comes with two Tegra system-on-chips (SoC) and two Pascal graphics processors, which have dedicated memory and specialized support for DNN calculations. In cases where more diverse tasks are required for autonomous driving, the MobilEye EyeQ5 [135] may be more suitable since it offers four fully programmable accelerators, each optimized for a different family of ML algorithms. This can be helpful in situations where various DL algorithms have been utilized. Alternatively, Altera's Cyclone V [135] SoC provides a driving solution that has been specifically optimized for sensor fusion. For a more detailed review of hardware platforms available for autonomous driving, please refer to the discussion by Liu et al. [122]. If the reader is interested in delving deeper into the analysis of certain simulators, they may refer to [210] for a more comprehensive examination.
- Datasets: The availability of various DL datasets for autonomous driving and perception has significantly increased due to the rapid progress in implementing DL systems on CAVs [110]. The authors [100], present an overview of the different vehicular IDS datasets according to the nine specific criteria. One of the most famous datasets for autonomous driving is the KITTI benchmark suite, which includes several datasets for evaluating stereo vision, optical flow, scene flow, simultaneous localization and mapping, object detection and tracking,

TABLE III
COMMON NON-SECURITY CHALLENGES IN SMART VEHICLES

Challenges	Key Points	Papers
High Mobility of Vehicles	Extensive mobility, highly dynamic topology, and vibrant nature of traffic result in short-lived connections and isolated clusters of nodes.	[48], [26], [68], [116]
Heterogeneous and Stringent QoS Requirements	V2V and V2X communications occur either periodically or in response to specific events, demand high reliability, and are very sensitive to delays	[116]
Dynamic Learning Environment	Sensors, cameras, GNSS, network topologies, and traffic dynamics	[224]
Distributed Representation of Data	Data is produced and stored across various units throughout the network, such as vehicles, roadside units, and cloud-based remote storage.	[224]
Network Congestion Control	Potential to cover vast geographic areas, ranging from a single city to multiple cities or even entire countries.	[223]
Time Constraints	Applications and services that operate under strict deadlines, such as navigation, traffic flow, congestion control, and efficient implementation of vehicular networks demand hard real-time guarantees	[220]
Integration Challenges with Emerging Technologies	AI, IoT, cloud computing, edge computing, and Blockchain	[78], [69], [206]

road detection, and semantic segmentation [72], [73]. There are also other helpful datasets such as Waymo Open [123], Oxford Robotcar [127], ApolloScape [90], Udacity [91], ETH Pedestrian [65], and Caltech Pedestrian [58] datasets. To get a comprehensive view of all the available autonomous driving datasets, you can refer to the survey conducted by Yin and Berger [225]. Additionally, apart from public datasets, there are also many different tools accessible for developing DL in CAVs.

IV. NON-SECURITY CHALLENGES IN SMART VEHICLES

The automotive industry is a multifaceted and ever-changing sector that has encountered several complications and concerns over the years. Some of the significant non-technological-related challenges and issues confronting the automotive industry involve safety [106], [163], environmental concerns, geopolitical issues, cultural differences, legal challenges, changes in labor markets, supply chain disruptions, surges in traffic congestion, elevated fuel costs, rise in Carbon dioxide discharges, and so on.

CAVs represent state-of-the-art technology in the realm of smart vehicles, offering a transportation option that is not only more efficient but also safer and more convenient. However, there are multiple challenges that exist, both security-related and non-security-related, that must be overcome to ensure the successful implementation of CAVs in the long run. CAVs technology presents diverse non-security-related challenges (summarised in Table III) as given below:

A. High Mobility of Vehicles

Due to the extensive mobility of CAVs in vehicular networks, there is a highly dynamic topology that creates a range of communication challenges for the networks. Moreover, the dynamic nature of traffic can cause network partitioning, resulting in isolated clusters of nodes (vehicles, roadside units, and infrastructure). The short-lived connections between vehicles and nearby roadside units result in a short wireless channel coherence time, making it difficult to achieve accurate real-time channel estimation at the receiving end. As a result, there is a need to develop dynamic and robust resource management protocols that can effectively utilize available resources while also adapting to variations in vehicular density [26], [48], [68], [116].

B. Heterogeneous and Stringent QoS Requirements

Vehicular networks employ various communication modes such as V2V and V2X communications. These types of communication, which may occur either periodically or in response to specific events, demand high reliability and are very sensitive to delays. As a result, designing wireless systems for CAVs requires meeting a range of heterogeneous and strict quality-of-service (QoS) requirements that cannot be met through conventional wireless design methods [116].

C. Dynamic Learning Environment

Vehicular networks are highly dynamic in various aspects, such as sensors, cameras, GNSS, network topologies, and traffic dynamics. Predicting and learning these dynamics effectively and reliably based on historical data from multiple sensors or previous transmissions are still an unresolved matter. In the past, various ML models have been utilized to characterize the temporal relationship and predict future states. However, new advanced models that leverage ANNs, such as RNN and LSTM, have shown promise in improving predictions by taking advantage of long-term dependencies [224].

D. Distributed Representation of Data

Data within vehicular networks are typically produced and stored across various units throughout the network, such as vehicles, roadside units, and cloud-based remote storage. To ensure the effective functioning of the system, it is important to take into account the additional overheads associated with coordinating and sharing information among various units in vehicular networks for distributed learning [224].

E. Network Congestion Control

Vehicular networks have the potential to cover vast geographic areas, ranging from a single city to multiple cities or

even entire countries. However, this expansive nature poses a challenge in the form of network congestion. This is particularly true in urban areas where traffic density is high, especially during peak hours, which can cause issues with network congestion [223].

F. Time Constraints

In order to serve as a reliable foundation for a variety of applications and services that operate under strict deadlines, such as navigation, traffic flow, and congestion control, efficient implementation of vehicular networks demands hard real-time guarantees [220]. As a result, it is important that critical information is broadcasted in a timely manner by either the vehicles themselves or roadside units.

G. Integration Challenges With Emerging Technologies

To create a reliable ITS, it is crucial to smoothly incorporate and interoperate with emerging technologies such as IoT, cloud computing [78], and Blockchain [69], [206]. This issue focuses on identifying and discussing the integration hurdles that must be overcome that the automotive industry encounters.

H. Additional Challenges

There are numerous issues associated with smart vehicles, and it is not feasible to address all of them in a single article. One relevant study is presented in [36] to overcome the issue of erratically positioned on-road objects, where the author examines the issue of trajectory optimization for autonomous vehicles while taking into account several maneuver phases and erratically positioned on-road objects. In [37], the author suggested a centralized robust model predictive control method for attitude tracking control in reentry vehicles. In [38], the author introduced a new approach called Dual-Loop Tube-Based Robust Model Predictive Attitude Tracking Control for Spacecraft. This method takes into account system constraints and additive disturbances.

V. Security Issues in Smart Vehicles

Cybersecurity pertains to the safeguarding of computer systems (Data, software, hardware) and networks against digital attacks. In 1977, a publication by NIST introduced the CIA triad, which stands for confidentiality, integrity, and availability, as a simple yet effective means of describing crucial cybersecurity objectives [174]. The CIA triad is still a valid framework that provides a useful way to think about the goals of security measures [143]. Confidentiality focuses on ensuring the privacy of sensitive information and processes from unauthorized access. Integrity is about maintaining the accuracy and consistency of data throughout its lifecycle and safeguarding it against unauthorized modifications or deletions. Availability aims to ensure that authorized users can access data and systems when required. Cybersecurity can be categorized into numerous types such as information, software, network, wireless, physical, mobile, cloud, endpoint, IoT security, and so on.

Security attacks refer to intentional actions carried out by individuals or groups to exploit vulnerabilities in computer systems or networks to compromise any one or more of the CIA triad. Security attacks arise in various forms, ranging from straightforward password attacks and phishing scams to more advanced malware infections and Distributed Denial-of-Service (DDoS) attacks. The significance of vehicle security has grown steadily due to the increased reliance on computer systems, wireless network standards, the Internet, and the proliferation of smart devices. This section presents some common attack surfaces and types of security attacks that smart vehicles may face. The visual depiction of this Section can be seen in Figure 7. In Figure 8 we demonstrated the block diagram of the attack surface of a smart vehicle.

A. Attack Surfaces of Smart Vehicles

The attack surface or attack vector of a smart vehicle refers to the collection of vulnerabilities, entry points, pathways, and techniques that can be exploited by an attacker to engage in a cyber-attack on the vehicle. The access channels through which smart vehicles can be targeted can be categorized into three primary types, comprising the attack surface: physical access, in the proximity (short range wireless access), and long range wireless access (remote access). Below are the attack surfaces about these categories that could be exploited to infiltrate a smart vehicle and execute malicious payloads:

1) Physical Access: Smart vehicles are vulnerable to digital attacks as they have several physical interfaces that can be exploited by attackers. These interfaces can provide direct access to the ECUs and IVNs (e.g., CAN and LIN buses) of the vehicle, making it easier for an attacker to infect the system and cause harm. One such interface is the OBD-II port, which is traditionally utilized by service professionals for diagnosing and programming ECUs during maintenance checks [107]. Smart vehicles are also vulnerable to providing physical access through their entertainment systems, which can be achieved by using physical sources like USBs, iPods, and CDs [41].

2) Short Range Wireless Access: The communication channels in smart vehicles within limited distances can be employed to exploit the security vulnerabilities such as sensors (e.g., LIDAR and RADAR), cameras, Bluetooth, RFID (remote keyless entry), Wi-Fi, and DSRC. Hackers can position a wireless transmitter in close proximity to the vehicle's receiver, depending on the channel distance, to carry out such attacks [41].

3) Remote Access: Digital access channels that cover long distances can be classified into two categories: broadcast channels and addressable channels. Broadcast channels, including GNSS, Traffic Message Channel, Digital Radio, and Satellite Radio are a type of indirect channels that are connected to other significant ECUs. Addressable channels refer to specific channels that utilize cellular networks and are accessible from any distance. However, these long-range wireless networks are susceptible to attacks by the remote transfer system that facilitates continuous connectivity through cellular voice and data networks [41].

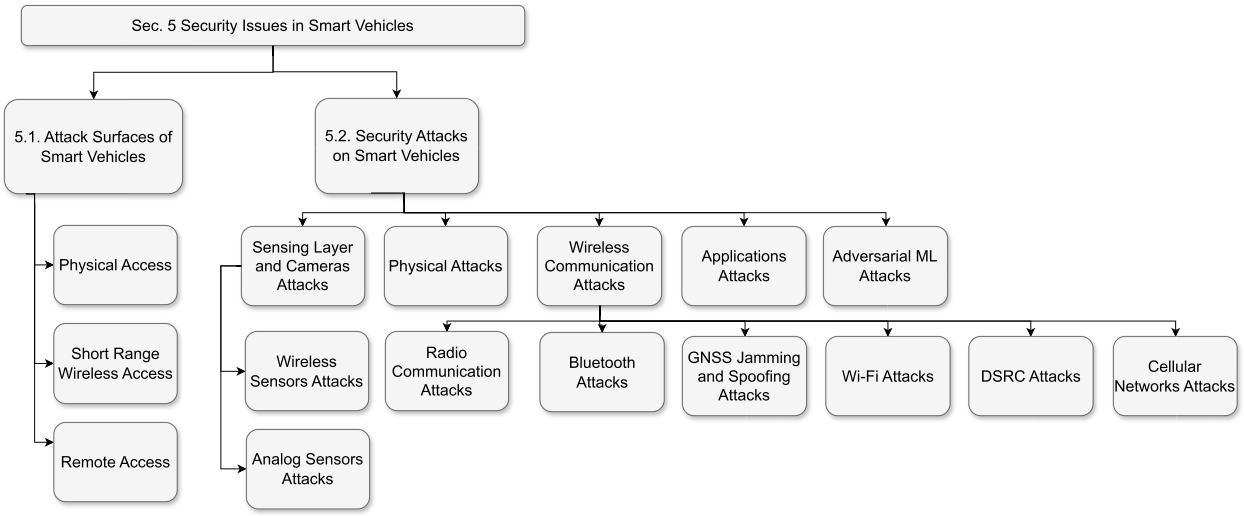

Fig. 7. The visual representation of security issues in smart vehicles (Section V).

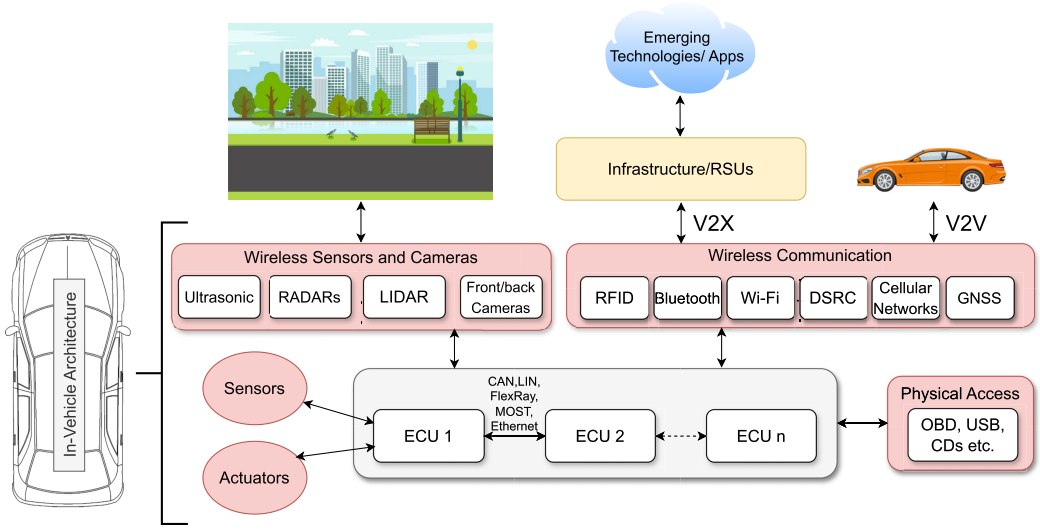

Fig. 8. The attack surface of a smart vehicle.

There are several ways in which attackers can exploit the above-mentioned attack surfaces in smart vehicles to launch security attacks [17], [63], [160]. For example, the automotive industry's recent advancements include incorporating the Human-Machine Interface (HMI) screen that enables integration with popular smartphone applications like Apple Car Play and Google Android Auto. However, these vehicle apps may lead to security breaches and provide an avenue for malicious attacks on the HMI, resulting in unauthorized access to vital vehicle functions. These automobile applications rely on wireless mobile telecommunication technologies such as cellular networks, Wi-Fi, and Bluetooth. Another example is the telematics system which provides information about various in-vehicle systems including vehicle speed, tire pressure, seat belts, door locking, fuel efficiency, transmission, and engine issues [94]. The telematics unit in modern vehicles enables communication with cellular networks, which can potentially allow attackers to gain access to the vehicle and carry out harmful actions.

B. Security Attacks on Smart Vehicles

The functionality of smart vehicles heavily relies on smooth and reliable V2X and in-vehicle communication. However, these communication systems are susceptible to numerous security attacks [136], [229]. In order to gain a comprehensive understanding of security attacks on smart vehicles, numerous classification attributes have been employed in the literature. These include the CIA triad [131], [193], OSI layers model [17], [160], functionality [156], as well as classifications based on factors such as whether the attack is direct or indirect [194], active or passive, external or internal, and malicious or rational [166]. We have distributed the top security threats for smart vehicles with regard to the attack surface and communication channels through which a vehicle can be targeted. We have compiled a list of the significant security threats affecting smart vehicles, concentrating on the major attack surfaces, and made an endeavor on correlating them with the CIA triad. Table IV summarized the significant security attacks affecting smart vehicles.

TABLE IV
LIST OF THE SIGNIFICANT SECURITY THREATS AFFECTING SMART VEHICLES

Attack Umbrella	Type of Attack	Paper
Physical Attacks (OBD-II port, USBs, and CDs) [107], [41]	Frame Sniffing	[103], [146], [228], [22], [107], [33], [22], [32]
	Frame Falsifying	[107], [133]
	Frame Injection	[107]
	Replay Attack	[107], [86]
	DoS Attack	[107]
Sensing Layer and Cameras Attacks	Wireless Sensors Attacks (ultrasonic, LIDAR, and RADAR)	[155], [217]
	Analog Sensors Attacks	[182]
Wireless Communication Attacks [227], [223]	RKES (Radio)	[185], [119], [56]
	TPMS (Radio)	[173], [173]
	Bluetooth Attacks	[150], [116]
	GNSS Attacks	[25], [201], [191], [202], [67], [154], [158], [60], [201], [191], [202]
	Hotspot, Open Wi-Fi, and Weak Encryption	[70], [139], [145], [139], [207]
	OBD Port Attacks through Wi-Fi	[104], [170], [171]
	DSRC Attacks	[211], [215]
	Cellular Networks Attacks	[148], [138], [134]
Applications Attacks	Sybil attacks	[221], [66]
	Botnet attacks	[71]
	Open-source software/MirrorLink	[96], [130]
Adversarial ML/DL Attacks [23]	Tweaking traffic signs and logos	[44], [19], [190], [189]
	Standard DL datasets used in adversarial research	[112], [108], [53], [112], [109], [187], [195], [83], [95]

1) Physical Attacks: A set of experimental studies has been carried out on in-vehicle network attacks [120]. Within this section, we will explore various forms of attacks that can be directed toward in-vehicle networks as given in [156].

- **Frame Sniffing** Due to CAN buses broadcast-based communication protocol and lack of designated sender and receiver addresses, each node within the network receives the frame without any Message Authentication Code (MAC) or digital signature [103], [146], which results in an unsecured transmission. The starting point for all attacks on in-vehicle communication is frame sniffing. CAN frames are sent to all ECUs, making it possible for a compromised ECU to intercept all frames transmitted through the CAN bus by accessing the in-vehicle network via available interfaces (such as the OBD port and USB ports), and aftermarket devices [22], [228]. By analyzing historically recorded frames, one can obtain details about the CAN frames. In [107], authors developed a custom program called CarShark, which was specifically designed to intercept frames and data sent by the CAN system. They discovered that the range of valid CAN frames is limited, enabling attackers to uncover various functions and weaknesses on selected ECUs. Moreover, By utilizing the OBD port, diagnostic data can be collected, the in-vehicle network can be accessed, and malware can be installed [22], [32], [33].
- **Frame Falsifying** If attackers have knowledge of a majority of valid CAN frames, they can craft their attacks by sending forged frames through the CAN bus. For instance, an attacker can manipulate fuel level readings, modify the speedometer readings, and display false failure information on the instrument panel cluster by altering frame data [107]. Valasek and Miller were able to establish communication over the CAN bus through an ECOM cable (CAN to USB converter) and custom-made connectors that were connected to the OBD port [133].
- **Frame Injection** A starting point for attackers could be a malicious node, which can take various forms such as a laptop connected to the OBD port infected with malware. The most severe case could involve a reprogrammed ECU, equipped with wireless or remote communication capabilities like Wi-Fi or Bluetooth. Typically, custom-built software is used in previous studies to inject frames into the network, and manipulating the frames' ID allows the fraudulent frames to be accepted by the targeted node on the CAN bus [107].
- **Replay Attack** The replay attack shares many similarities with the previously described attacks. By utilizing the malicious node, attackers are able to issue commands for legitimate frames to be sent to the CAN bus at specific times. This means that if the vehicle is stationary, an attacker can use this technique to unlock the doors, turn on the engine and lights, and drive away by injecting

valid CAN frames into the vehicle's in-vehicle network. Koscher et al. demonstrated that a replay attack can be executed in a real-world car scenario [107], while Hoppe and Dittmann conducted simulations to explore the implementation of a replay attack in related work [86].

- **DoS Attack** The frame ID that determines the order of frame transmission on the CAN bus also creates the possibility for DoS attacks, where attackers can issue commands to the malicious node to continuously broadcast high-priority frames. This effectively blocks other nodes from transmitting their frames as long as there is a higher-priority frame in the network. Koscher et al. demonstrated this vulnerability in [107], where they employed a DoS attack to disable communication between specific components on the CAN bus.

2) Sensing Layer and Cameras Attacks: The sensing technology utilized by smart vehicles encompasses a range of sensors including ultrasonic, RADARs (SRR, MRR), LIDAR (LRR), and forward and backward cameras. Various computer vision techniques, including modern ML/ANN-based methods, are utilized to develop the perception system of CAVs. This system is responsible for identifying objects such as pedestrians, traffic signs, and symbols. However, it is highly susceptible to physical world conditions and adversarial attacks on the sensory layer [155]. For instance, to predict the steering angle and brakes based on sensor or camera input. This section provides a concise overview of the potential security attacks that target the sensing layer and cameras.

a) Wireless Sensors Attacks: In Defcon24 back in 2016 [217], a demonstration was carried out focusing on the sensors that guide driving, such as RADARs, ultrasonic sensors, and forward-looking cameras. They have conducted contactless attacks on these sensors and collected data using Tesla, Audi, Volkswagen, and Ford vehicles. Their findings indicate that off-the-shelf hardware can be used to perform jamming and spoofing attacks, which can cause malfunctions and blindness in Tesla's sensors. These issues have the potential to cause accidents and compromise the safety of self-driving cars. To address these concerns, they also propose software and hardware countermeasures that can improve the sensors' resilience against such attacks. Specifically, the researchers demonstrated that these attacks are to create sounds that result in prolonged vibration of the sensor's membrane, rendering accurate measurements impossible. When obstacles aren't detected due to this interference, it can result in collisions while parking or maneuvering.

The paper [155] presents evidence of successful jamming, spoofing, blinding, and replay attacks on two perception systems of smart vehicles, specifically the camera and the LIDAR, and preventive measures to counteract these attacks. These attacks are carried out by using various techniques. For instance, in a blinding attack, the attacker obscures the camera either completely or partially by projecting light onto it, with the aim of concealing objects. In a replay or relay attack, the attacker strives to retransmit the initial signal sent by LIDAR to the target vehicle using another position. The objective is to fabricate false echoes, which can cause genuine objects to appear either nearer or farther than their genuine locations. The attacker can execute these attacks by installing the necessary hardware on another vehicle to launch an attack. Once installed, the attacker can drive the vehicle in front of, behind, or next to the target vehicle for carrying out the attack. In addition, the attacker makes use of stationary attack sensors situated by the side of the road, for instance, the guard rail.

b) Analog Sensors Attacks: An attacker can manipulate the physical environment surrounding analog sensors, like ABS to exploit vulnerabilities in wheel speed sensors. This exploitation could potentially lead to dangerous situations. ABS relies on magnetic-based wheel speed sensors that can be accessed by an external attacker from underneath a vehicle's body. In [182], the researchers show how an attacker can use a thin electromagnetic actuator near the ABS wheel speed sensors to cancel out the true measured signal and inject a malicious signal.

3) Wireless Communication Attacks: The use of wireless communication technologies like Wi-Fi, DSRC, cellular networks, and Bluetooth in smart vehicle applications enables communication with the vehicle. However, this also means that smart vehicles become an open system, which poses a potential threat [223], [227].

a) Radio Communication Attacks: Smart vehicles employ radio frequency communication to remotely control various functionalities, including opening and starting the vehicle, tire pressure monitoring, controlling lights, and activating alarms.

- **Remote Keyless Entry and Start (RKES):** In RKES system, the key fob plays a crucial role in controlling various aspects of a vehicle, including locking and unlocking doors, controlling power windows, operating the ignition, and managing the alarm system. To achieve this, the key fob transmits encrypted radio signals, which are decrypted by the smart key ECU. The decrypted data is then matched against previously stored information to authenticate the key fob. Once authenticated, the key fob is connected to the IVNs. The attack on an RKES can occur within a 100-meter radius, where the hacker can clone or relay the key's signal and gain access to the vehicle in under two minutes [185]. Researchers such as Liu et al. [119] have demonstrated various attacks that can exploit vulnerabilities present in the Hitag2 cipher, widely used in remote keyless entry systems. In another instance, Dibaei et al. [56] were able to steal a Mercedes-Benz vehicle by manipulating its keyless entry system with just two hackers.
- **TPMS:** is a self-contained unit that constantly monitors the pressure levels of tires. It is governed by a separate ECU and utilizes radio signals to communicate with the TPMS module in the event that tire pressure dips below safe parameters. According to [173], many hobbyists mishandle systems by tampering with the TPMS, which can result in false readings being sent out to create fake warnings and cause confusion for drivers. In [173], a privacy and security assessment of TPMS is conducted through both laboratory experiments involving isolated tire pressure sensor modules and experiments carried out on a complete vehicle system. The findings reveal that

eavesdropping can be accomplished with relative ease from a distance of approximately 40 meters as a vehicle passes by.

b) Bluetooth Attacks: Most smart vehicles currently support Bluetooth technology, offering a 10-meter range for wireless connectivity. Commonly used to link cell phones with a vehicle's infotainment and telematics system, it enables drivers to make calls and stream music. Attacks such as eavesdropping, data theft, and unauthorized access can be carried out on Bluetooth technology itself, leaving it vulnerable. An attacker may connect their smartphone to the vehicle's Bluetooth and upload malicious code into the system. To prevent such attacks, it may be necessary to implement confirmation Bluetooth connectivity on the infotainment system, making it more challenging for hackers to establish a Bluetooth connection [114], [150].

c) GNSS Attacks: The act of blocking and spoofing GNSS signals is typically carried out by cybercriminals to compromise authenticity and integrity [25], [191], [201], [202]. It's worth noting that the sale or use of equipment designed to intentionally disrupt communication signals, including GNSS jamming equipment, is against the law in many countries worldwide. However, it's also possible to conduct GNSS jamming using legal inexpensive SDR (Software Defined Radio) technology [67], [154]. According to [158], advanced spoofing techniques have smart vehicles susceptible to GNSS signal spoofing, which highlights the need for continued investigation into this issue. GNSS spoofing allows hackers to manipulate the data of navigation systems without the operators being aware of the interference which results in malicious navigation and weather information. In GNSS spoofing attack, the attacker uses a radio transmitter, such as SDR, to transmit a fake GPS signal to a receiver antenna. The purpose of this is to disrupt the legitimate GNSS satellite signal. This type of attack works by overriding the weaker, genuine satellite signal with the stronger, false signal. While it is possible to achieve GNSS spoofing using a simulator that generates a fake satellite signal [60], [191], [201], [202]

d) Wi-Fi Attacks: With over 75% of the Internet traffic in the last mile being carried by Wi-Fi, it has become an attractive target for various security threats [70].

- **Hotspot, Open Wi-Fi, and Weak Encryption:** Smart vehicles are equipped with Wi-Fi, allowing them to connect to internet hotspots or open Wi-Fi within range. However, some of these hotspots may pose a risk due to outdated encryption standards that can put the vehicle's security at risk. The initial encryption standard for wireless networking devices, Wireless Encryption Protocol (WEP), has been considered weak and vulnerable to hacking. Wi-Fi Protected Access (WPA) was meant to replace WEP, but it too has been found to have flaws [139]. Moreover, fake Wi-Fi hotspots may expose vehicles to malicious attacks. For instance, hackers can remotely take control of a Tesla vehicle by exploiting vulnerabilities in how the secret key to an installed Wi-Fi is saved in plain text [145]. Additionally, attackers can eavesdrop on Wi-Fi activity by connecting to an illegitimate Wi-Fi access point [139]. Another research has shown that WPA is also vulnerable to DOS attacks [207].
- **OBD Port Attacks through Wi-Fi:** Despite the OBD dongle being traditionally a physical connection to the OBD port, vehicle manufacturers are now incorporating Wi-Fi technology to allow access to the OBD port through a computer. This advancement in technology permits hackers to perform an array of activities on the vehicle, including but not limited to locking and unlocking doors, starting and stopping vehicles via the push button, making steering adjustments, and braking, among other things [104]. A bash script was utilized by researchers to establish a long-lasting connection with Mazda's infotainment system through the vehicle's Linux operating system [170]. By taking advantage of an exposed port, the researchers were able to gain access to a vehicle's infotainment system through the vehicle's Wi-Fi connection. Additionally, another research team managed to remotely access the address book, conversation history, and location data by connecting to the root account of the infotainment system [171].

e) DSRC Attacks: DSRC is a technology that enables V2V and V2I communication over short distances. This can be incredibly useful for improving safety and efficiency on the roads, but it also presents some security risks. It is imperative to give due consideration to implementing stringent safety measures for safeguarding V2V and V2I communications as highlighted in references [211], [215].

f) Cellular Networks Attacks: Cellular networks are at risk of security breaches such as sniffing and jamming attacks. Cichonski et al. discovered that even LTE networks can be hacked with relative ease using these methods [148]. Vehicular networks based on LTE and 5G technologies are particularly susceptible to a wide range of attacks, which could allow malicious actors to track vehicles and potentially carry out harmful operations [138]. For instance, a Jeep Cherokee running on a highway was remotely hacked and brought to a stop through 4G connectivity by Miller and Valasek [134].

4) Applications Attacks: Although technologies that enable precise control of vehicles have enhanced drivers' safety and convenience, their weaknesses have also been scrutinized and taken advantage of. Despite this, open platforms like the Android OS have been integrated into vehicle systems without adequate attention to potential security problems [96]. The focus of this paper [96] is to highlight security issues with a telematics system based on the Android OS. The firmware for the device is readily available on a public website, making it vulnerable to analysis using commonly available tools. In addition, a situation is described where hackers acquire OTA firmware and subsequently include techniques for controlling the vehicle from a remote location. In [130], authors revealed that the MirrorLink protocol, which connects smartphones to vehicle infotainment systems, can be exploited by attackers to enter the CAN bus system and introduce harmful messages.

In [71], the researcher presented a botnet attack that utilizes VANET technology and targets road segments. This form of attack can lead to significant physical traffic congestion issues. Their attack involves the parked bot vehicles that are stationed

TABLE V
SUMMARY OF THE SECURITY MEASURES AGAINST THE SECURITY ATTACKS ON SMART VEHICLES

Category of Solutions	Solution	Methodology	Papers
Cryptography	Protection against replay attacks	AES encryption for securing the CAN frames	[213]
	Securing CAN-Bus in agricultural technology	Application of Tiny algorithm to encrypt data	[98]
	Securing real-time communication of IoVs	EAST (combination of encryption and steganography)	[164]
Authentication & Privacy Preserving	Frame level authentication	Transmit message authentication code using separate frames	[147]
	Authentication and privacy protection	CPPA scheme specifically designed for VANET environments	[82]
	Remote attacks on the in-vehicle (CAN)	Zero-knowledge identification scheme	[81]
Signal-Processing-Based Techniques	Protection against GNSS spoofing attacks	Signal processing algorithm integrated into a basic GNSS receiver	[158]
	Security attacks on LIDAR	Utilizing multiple wavelengths	[129]
	Protection against GNSS spoofing attacks	Determining the minimum signal precision	[203]
Anti-Malware & Firewalls	Malware attacks detection	Anti-virus software and firewalls	[193], [184], [47]
Certificate Revocation	Securing modern vehicles	Certified and thoroughly tested apps	[130], [167]
Other Solutions	GNSS spoofing attacks	Utilization of onboard ADAS sensors to identify instances of GNSS	[117]
	Security attacks on RADARs	Data fusion	[218]
	Provide traffic safety	Shifting the RADAR frequency to a higher range	[105]

in various locations and carries out malevolent activities by promoting false physical traffic congestion details through advertisements. To carry out VANET experiments, researchers utilized Veins, which is an integration of SUMO and OMNeT simulators.

In a V2V communication, a Sybil attack involves the use of multiple active fake identities (also known as Sybil identities) that are operated by a single node (i.e., vehicle) simultaneously. These fabricated characters can be employed to launch various attacks on the network [221]. Additionally, they create an illusion of an increased number of vehicles on the roads, accidents, or traffic jams that may endanger the safety of individuals who are on the move [66].

5) Adversarial ML/DL Attacks: Although ML techniques have demonstrated exceptional performance in various applications, such as achieving human-level accuracy in image recognition, they still display significant susceptibility. Adversarial ML attacks can be defined as inputs to the ML or DL models that are created or manipulated by an attacker. The attacker adds a small and subtle change in the input, which is usually undetectable to humans, but it can compromise the accuracy and reliability of the ML/DL model. Adversarial ML attacks have the potential to occur either during the training or testing phase of an ML model. A poisoning attack, which is an adversarial attack during the training phase of ML, occurs when an attacker manipulates the training data to compromise the ML/DL model [23].

On the other hand, an evasion attack is an adversarial attack during the inference phase of the learning process where an attacker manipulates the test data or real-time inputs to produce a false result from the deployed model. In [160], the main emphasis of the researchers lies in analyzing adversarial attacks on CAVs and proposing a solution to safeguard against such attacks in various scenarios. In [44], the authors maliciously designed input data for sensors with the specific objective of influencing ML policies. Several researchers demonstrated an actual adversarial ML attack that involved tweaking traffic signs and logos with adversarial perturbations [19], [189], [190]. The standard DL datasets that are frequently used in adversarial ML research include MNIST [112], CIFAR-10 [108], and ImageNet [53]. In terms of evaluating adversarial examples, victim ML/ANN models such as LeNet [112], AlexNet [109], VGG [187], GoogLeNet [195], CaffeNet [95], and ResNet [83] are commonly employed.

VI. SOLUTION AGAINST SECURITY ATTACK

In this section, we focus on the different methodologies, network technologies, and protocols categorically discussed in the literature and compiled a list of the security measures that have been implemented against the security threats on smart vehicles. The table V provides a summary of the security measures implemented in the literature to protect smart vehicles against security attacks. Figure 9 displays a graphical illustration depicting this Section.

A. Cryptography

When dealing with a malicious outsider intending to launch cyber-attacks, particularly application layer attacks, utilizing cryptographic methods can be a useful and effective preventive measure [131]. In their study, Woo et al. [213] suggested a security protocol that utilized AES encryption for securing the

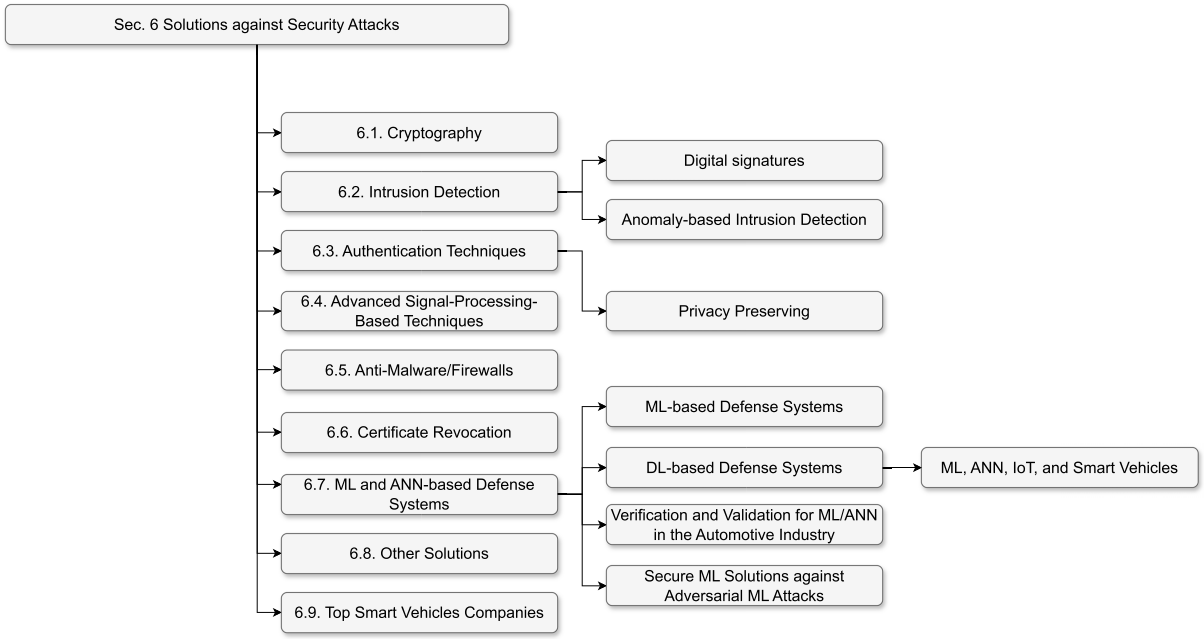

Fig. 9. The visual representation of listed solutions against security attacks on smart vehicles (Section VI).

CAN frames. The protocol achieved robustness against replay attacks by expanding the ID field and the 16-bit CRC field that is commonly used to verify the identity of the transmitted ECU. Additionally, the protocol incorporated a counter for recording frame generation. The article "GNSS Spoofing and Detection" discovered that encryption-based defenses can detect and prevent spoofing attacks on GNSS in smart vehicles, which prove challenging for any potential spoofer to replicate without resorting to a meaconing attack. [158].

The main focus of [98] article is to examine the potential use of the Tiny encryption algorithm on the CAN-Bus (especially in agricultural technology) for recognition and implementation purposes. The goal is to assess how effective the Tiny algorithm is in encrypting data on the 250 kbit/s CAN-Bus. Another study focused to improve the security of data during real-time communication in the realm of the IoV. The approach taken involves a privacy technique that prioritizes trust, utilizing encryption and steganography within the IoV system. This strategy utilizes an algorithm called Efficient Algorithm for Secure Transmission (EAST) which combines both encryption and steganography algorithms [164].

B. Intrusion Detection

Intrusion detection systems mainly utilize two methods for threat detection - signature-based and anomaly-based, as given below:

1) Digital Signatures: Digital signatures also offer a reliable solution for preserving the authenticity and confidentiality of messages, shielding them from potential unauthorized usage [14]. When the signatures-based IDS detects patterns in observed events that match known attack patterns (signatures), it reports an intrusion. This approach has limitations in detecting new types of attacks such as zero-day attacks. Also, keeping the signatures database up-to-date is a challenging task, especially with the constant emergence of new attack types.

2) Anomaly-Based Intrusion Detection: As the presence of a trusted but compromised vehicle with a valid certificate poses a challenge to protecting against security threats, data-driven anomaly detection methods can be employed in such situations. In [126], [162], and [205], the researchers provide information and the survey on enhancing the security of connected vehicles through the anomaly. Additionally, in order to identify instances of the selective forwarding attack, a trust system approach is proposed in [208]. This method involves the monitoring and detection of abnormal driving patterns through both local and global detection of attacks among internodes. To simulate the movement of vehicles, MATLAB is utilized. ML plays a critical role in anomaly detection. Common applications of anomaly detection via ML are discussed in Section VI-G.

C. Authentication Techniques

By utilizing suitable authentication and detection techniques [178], it is possible to reduce the impact of security attacks on smart vehicles. Nilsson et al. suggested in [147] a method for transmitting a message authentication code using separate frames. By dividing the 64-bit MAC into four 16-bit sections, it can be sent in four distinct frames. This approach has the potential to enhance the efficiency of transmitting authenticated frames.

Broadcasting the traffic status messages to vehicles can enhance traffic safety and efficiency through the use of a VANET. However, for secure communication within VANETs, it is necessary to address security and privacy concerns before their implementation. The conditional privacy-preserving authentication (CPPA) scheme is well-suited for addressing security and privacy concerns in VANETs as it offers both mutual authentication and privacy protection. In recent years,

several identity-based CPPA schemes have been proposed for VANETs that use bilinear pairings to improve security and performance. However, the bilinear pairing operation is known to be highly complex in modern cryptography, which creates computational challenges when processing information in VANETs. As a solution to this problem [82], the researchers present a novel CPPA scheme specifically designed for VANET environments that does not rely on bilinear pairings. Their proposed scheme demonstrates that it can effectively support both mutual authentication and privacy protection simultaneously.

In [81], the researchers devised a secure and effective identity authentication system utilizing the Feige-Fiat-Shamir (FFS) zero-knowledge identification scheme with excellent soundness. This was achieved by taking into consideration the remote attack model for vulnerabilities of the in-vehicle CAN. They incorporated the techniques of zero-one reversal and two-to-one verification to address the issue of FFS being susceptible to guessing attacks.

1) Privacy Preserving: One way to address the risk of data interception attacks is to implement the access control models [79] and privacy-preserving techniques based on authentication methods [118], [177]. According to a simulation study [43], researchers have developed a software-based solution that utilizes two shared secrets to meet the privacy requirement. This solution has a lower message overhead in the message verification phase compared to previous solutions.

D. Advanced Signal-Processing-Based Techniques

Signal processing techniques are widely used in vehicle security to detect and prevent attacks especially the attacks on sensors. In [158], signal processing techniques-based solution is discussed for detecting spoofing attacks, which can be integrated into a basic GNSS receiver in smart vehicles as advanced signal processing algorithms. This technique involves identifying anomalies that generally arise by attackers during signal drag-off, where distortions or disruptions are observed. Another type of defense (i.e., signal-geometry-based defense) against spoofing involves monitoring the direction from which signals arrive by analyzing the phase of the beat carrier that is received.

Potential security attacks can also be thwarted by utilizing various wavelengths. When multiple wavelengths are employed, such as with LIDAR technology, it becomes considerably more difficult for attackers to target both signals simultaneously [129]. As a result, the attacker has a larger budget, so the probability of an attack decreases. Another solution proposed for preventing GNSS spoofing involves determining the minimum signal precision required in order to successfully spoof these types of receivers [203].

E. Anti-Malware/Firewalls

A malware attack refers to the use of malicious or intrusive software such as computer viruses to compromise the network or software components of a system CAVs and Road Side Units (RSUs) [193]. To prevent such attacks, it is recommended to use anti-malware software and firewalls [47], [184].

F. Certificate Revocation

To prevent injection attacks from exploiting smartphone technology and gaining access to a vehicle's internal systems, it is crucial for manufacturers to ensure that only certified and thoroughly tested apps are permitted to establish a connection [130].

Vehicular networks rely on a certification authority to manage the identities and credentials of all vehicles in the system by issuing them valid certificates. Without a valid certificate, vehicles cannot operate within the network. To ensure security, certificates must be revoked after a specific period of time. However, the revocation process is challenging administratively because it involves identifying nodes with fraudulent behavior and changing the registered domain. Additionally, the revocation of malicious nodes' certificates is necessary to prevent them from attacking the system. Three distinct certificate revocation procedures have been put out to address these issues [167].

G. ML and ANN-Based Defense Systems

ML and ANN techniques are now widely used in a variety of automotive applications, such as traffic flow prediction [132], 3D object detection [87], fault diagnosis [169], vehicular security [100], [214], and many more. In this section, we will examine vehicle-specific IDSs based on ML and ANN in this part [8], [21], [124]. To solve the security issues in smart automobiles, a number of security professionals have created and tested IDS systems that depend on ML and ANN. Table VI lists all of the ML/DL-based security safeguards used in the literature to protect smart vehicles from security intrusions.

1) ML-Based Defense Systems: Anomaly detection can be performed by analyzing the order of messages transmitted from an ECU. These messages are sent in a specific sequence based on their priorities, and any deviation from this sequence can indicate an anomaly. Many algorithms have been proposed for this purpose [140]. In [13], the researchers introduce a set of ML techniques that utilize KNN and SVM algorithms for clustering and classifying intrusions in VANET. The intrusion detection approach is based on analyzing the offset ratio and time interval between message requests and responses in the CAN network. In their analysis, they utilized two car-hacking datasets - the "DoS dataset" and "fuzzy dataset" - which were supplied by the Hacking and Countermeasure Research Lab (HCRL) [1]. In [141], Narayanan and colleagues proposed an anomaly detection system that analyzes message streams originating from various ECUs. They treated these streams as sequences of events and transformed them into a time series ML problem. Subsequently, they employed Hidden Markov Models to construct a model representing typical behavior. For dataset collection, they attached a device to the OBD port of manufacturers such as Toyota, Honda, and Chevrolet in order to extract data.

Alheeti et al., have expanded their intrusion detection techniques in [10] to include measurable properties derived from sensors like magnetometers found in autonomous vehicles. To achieve this, they employed the Integrated Circuit Metrics (ICMetric) technology, which is capable of uniquely

TABLE VI
SUMMARY OF THE ML/DL-BASED SECURITY MEASURES AGAINST THE SECURITY ATTACKS ON SMART VEHICLES

Solution	Dataset	Methodology	ML/DL Model	Paper
IDS	DoS and fuzzy dataset	Clustering and classifying intrusions in VANET	KNN, SVM	[13], [1]
Anomaly detection	Collect data from vehicles (Toyota, Honda, and Chevrolet, etc.) through OBD port	Analyzed ECU's message streams	Hidden Markov Models	[141]
IDS	Extracted data from multiple identical sensors	Identifying system's behavior through magnetometer and gyroscope sensors reading	KNN	[10], [9]
Relay attacks on PKES	Three months log of PKES	Validate driver's loc through key fob features	Decision tree, SVM, and KNN	[5]
Anomaly detection	BigNetData dataset	Learn normal behavior from multivariate time series	SVM	[200]
Detect DoS and fuzzing attacks	CAN bus intrusion dataset v2	Identify abnormalities in vehicular systems	ANN (two dense layers (five neurons in each), activation function: Relu, output layer: SoftMax)	[20], [59]
IDS	CAN communication on OCTANE simulator	Utilizes ECUs packets features to distinguish normal from malicious traffic	Deep Neural Network (ReLU)	[99]
Anomaly detection	CAN data (extracted through OBD II port)	Predict next packet data and identify intrusions	LSTM-RNN	[198]
Vehicle theft	12 driving trips of 5 minutes from a driver	Identify drivers based on their real-world driving pattern	LSTM-RNN	[6]
GNSS spoofing attacks	comma2k19 driving dataset	Anticipate the distance moved between two consecutive locations	LSTM-RNN	[51]
Identifying gray holes and rushing attacks	ns-2 simulator based generated	Identify vehicle's behavior as normal or malicious	SVM and Feed-Forward Neural Networks	[11]
Hide IDS's features to enhance its performance	Extracted from three distinct car brands	Converting the data into an image using an encoder in real-time	CNN	[80]

identifying a system's behavior. Specifically, they integrated the bias reading of magnetometer sensors into the cyber features used in their previous work and employed a simple ML method based on k-nearest neighbors to identify anomalous conditions. They evaluated their approach using measurements from a real sensor system and an NS-2 simulation of the rest of their setup. In addition, in [9], they extended their evaluation to include the use of gyroscope sensors, which produced similarly positive results. They extracted data from multiple identical sensors.

In [5], researchers introduce a blend of ML approaches that aim to alleviate the negative impact of relay attacks on Passive Keyless Entry and Start systems. Their proposed algorithm capitalizes on key fob features to accurately profile the PKES system and driving features to identify the driver. Initially, the algorithm detects any relay attack; if none is detected, it unlocks the vehicle and leverages neural networks to verify the identity of the driver by obtaining their driving features. To evaluate the effectiveness of our model, we compared the performance of the decision tree, SVM, and KNN methods. Theissler et al. introduced a technique in the automotive setting that employs a radial basis function kernel-based one-class SVM to train on typical behaviors and detect anomalies as deviations from this learned baseline [200]. Experiments were conducted on the BigNetData dataset, which is a relational network traffic dataset.

2) DL-Based Defense Systems: Vehicle control can reap numerous advantages from DL [209]. The technology's capacity to analyze data and modify its actions according to new situations makes it highly effective in managing complex and dynamic environments [64], [165]. In [20], a DL-based lightweight IDS has been proposed to identify abnormalities in vehicular systems using a CAN dataset [59] obtained from real-time IVN communication protocol. The model effectively categorizes various attacks on vehicles, such as reconnaissance, DoS, and fuzzing attacks. In their ANN model, they utilized a sequential approach to construct a neural network, where we incorporated two dense layers, each consisting of five neurons and the input features size. The activation function used predominantly is 'Relu'. For the output layer, we specified the label's size and implemented the 'SoftMax' activation function. Kang and Kang presented DL-based IDS [99], which utilizes low-dimensional features extracted from IVN packets transmitted between ECUs to distinguish normal from malicious traffic. Particularly, they analyzed the probability of each class in discriminating between normal and attack CAN bus packets, the ANN can identify any malicious attack on the vehicle, thereby enhancing its security. The proposed method has demonstrated high detection accuracy

(99.8%) with real-time response capability against attacks. For dataset collection, the CAN bus receives packets that are generated by a simulator called Open Car Test-bed and Network Experiments (OCTANE).

Taylor et al. suggested an anomaly detector based on LSTM RNN, which achieves low false alarm rates in detecting attacks without requiring knowledge of the specific protocol [198]. This technique uses neural networks for predicting the next packet data and identifying intrusions. Their research is founded on a dataset gathered from a high-speed bus of a Subaru Impreza manufactured in 2012. By utilizing a USB-CAN bus interface connected to the vehicle's OBD II port, they acquired around 19 hours' worth of driving data. The authors employed LSTM-RNN to identify drivers based on their real-world driving data obtained from multiple routes under different traffic conditions [6]. The initial step involves checking for any relay attack, and only if none is detected, the vehicle is unlocked. After that, the algorithm proceeds with capturing the driving features and utilizing neural networks to verify the claimed identity of the current driver.

In [80], the proposed CNN-based system called CVNNs-IDS aims to hide features of an IDS and achieve a high level of accuracy in detecting attacks on the IoV. This is achieved by converting the data (CAN messages) into an image using an encoder in real-time, and then mapping it into the complex domain while simultaneously rotating it to reconstruct the authentic features. They extracted datasets from three distinct car brands and encompasses various datasets such as the fuzzy, flood, malfunction, replay attack datasets, and standard driving datasets.

In [51], the researchers have created a strategy for detecting GNSS spoofing attacks by utilizing the LSTM-RNN. The DL model is employed to anticipate the distance moved between two consecutive locations of an autonomous vehicle. To build the LSTM prediction model, a publicly available real-world comma2k19 driving dataset was employed, which contained different features like acceleration, steering wheel angle, speed, and distance traveled between two consecutive locations extracted from CAN, GNSS, and sensors of CAVs. Based on the predicted distance between the current and future locations of an autonomous vehicle, a threshold value is established using the positioning error of the GNSS device and the prediction error related to the maximum absolute error. The study concludes that their prediction-based strategy can successfully detect spoofed attacks on GNSS in real-time. Alheeti et al. have put forward an intelligent intrusion detection system for identifying gray holes and rushing attacks [11]. In order to design the IDS, both SVM and Feed-Forward Neural Networks (FFNN) were utilized to identify the vehicle's behavior as normal or malicious. The ns-2 simulator is used to create the dataset.

The geographic location of a smart vehicle station is considered personal data and is recorded with a signature. Attackers can exploit the V2V communication system to monitor a vehicle's CAM trace without proper safeguards. To protect the privacy and prevent misuse of collected information, selective communication approaches should be chosen over the continuous transmission of current CAMs. The researchers proposed GNN-based VANET topology learning methodology that emphasizes anonymity and can utilize any available Graph Learning framework [49]. Road traffic data is not strictly periodic and can be difficult to capture accurately. To address these challenges, the researchers [55] introduce CRFAST-GCN - a multi-branch spatial-temporal attention graph convolution network for the prediction of road traffic volume.

Based on reinforcement learning, the author developed a quick trajectory-planning method [35]. Additionally, they carry out the experimental validation of mobile robots in uncharted territory. In [34] and [39], the author put forth the idea of designing and implementing a deep neural network-based control system for the automatic parking maneuver process.

3) ML, DL, IoT, and Smart Vehicles: The widespread adoption of IoT technology has undoubtedly impacted the operational processes and procedures in intelligent transportation systems. In [157], the researchers propose a multi-agent system where each agent utilizes a Graph Neural Network to leverage the collaborative and cooperative abilities of intelligent agents for detecting anomalies. They present a distributed detection scheme to effectively monitor the entire network infrastructure against cyber-attacks, such as DDoS, which tend to spread rapidly. In [31], they investigated IoT home environments and identified vulnerabilities of the IoT gateways in the corresponding TCP/IP networks through DoS attacks, and in wireless networks through Denial-of-Sleep attacks. By analyzing packets captured from the PPP interface, they extracted statistical data samples to create a dataset and trained a dense RNN with it. Yavuz et al. [222] conducted a simulation of an IoT network testbed using the Contiki operating system. The researchers employed a DL method to detect Routing Attacks and used Random Decision Trees in combination with the Pearson coefficient correlation to extract the necessary data from the raw sensor data. The solution [4] being suggested utilizes an innovative sensor pairing method to assess the reliability of sensor data from IoT nodes by employing several ML models. Table VII lists the significant Challenges in the adoption of ML/DL technology into smart vehicles.

4) Verification and Validation for ML/ANN in the Automotive Industry: The use of ML/ANN is set to become a fundamental aspect of CAVs, but this also poses new challenges for safety evaluations. The certification of autonomous systems under the automotive safety standard ISO 26262 can be challenging as some of its critical aspects are not adequately defined. Certain process requirements may conflict with the nature of developing ML-based systems, particularly concerning Verification and Validation [84], [176]. To address this issue, the paper [28] evaluates the most current methods for verifying and validating safety-critical systems that employ ML/ANN.

Over a decade ago, the utilization of ANNs in flight controllers was a subject of active research, with a focus on ensuring adherence to strict aerospace safety standards. Presently, with the rise of autonomous driving, the researchers suggest [159], [199] that the automotive industry should gain insights from guidelines and the experiences gained from the verification and validation process of ANN-based components

TABLE VII
SIGNIFICANT CHALLENGES IN THE ADOPTION OF ML/DL TECHNOLOGY INTO SMART VEHICLES

Challenges	Paper
ML, DL, IoT, and Smart Vehicles	[157], [31], [222], [4]
Verification and Validation for ML/ANN in the Automotive Industry	[176], [84], [28], [159], [199]
Secure ML Solutions against Adversarial ML Attacks	[160], [75], [89], [152], [85], [125], [76]

developed to meet the DO-178B software safety standard for airborne systems.

5) Secure ML Solutions Against Adversarial ML Attacks: The defenses can be categorized against adversarial attacks into two main groups. The first group involves detecting the adversarial inputs after training ML models, while the second group focuses on proactively ensuring the ML model's robustness against such attacks [160]. Additionally, these techniques can be broadly classified into three categories: modifying data [75], [89], adding auxiliary models [85], [152], and modifying existing models [76], [125].

H. Other Solutions

Below are a few examples of other solutions available.

- A proposal was put forth in a recent study [117] suggesting the utilization of onboard ADAS sensors to identify instances of GNSS spoofing attacks in vehicular networks.
- The reference [105] supports the idea that the radar's accuracy could be enhanced by shifting the frequency from the 76.5 GHz band to a higher range beyond 100 GHz in order to enhance the traffic safety.
- The use of filters and alternative data sources, such as camera images, can be effective in reducing the impact of both replay attacks and RADAR/LIDAR confusion caused by reflective materials.
- An algorithm for data fusion was suggested in [218] to counteract security attacks of RADARs, making it more challenging to inject and jam signals while improving the detection of incoming attacks.

I. Top Smart Vehicles Companies

Currently, an increasing number of companies and research institutions are putting their resources into the development of CAVs. Noteworthy names in this field include Tesla, Google, Apple, BMW, Audi, Nissan, General Motors, Mercedes, Ford, Toyota, Honda, Volkswagen, and Nvidia, all of which have actively engaged in the research and development of autonomous vehicles [77].

With its strong foundation in AI, Google - an internet giant - is one of the forerunners in the self-driving car industry [24]. In June 2015, two of its autonomous vehicles were tested on actual roads and have since completed over 3.2 million kilometers of testing, making them the closest to real-world applications. Another significant player in this field is Tesla, which was the first company to implement self-driving technology in its production models. Through its "autopilot" feature, the company has achieved notable advancements in recent years. Although the National Highway Traffic Safety Administration (NHTSA) considers Tesla's autopilot technology only at Level 2 stage, it remains one of the most successful companies in applying this systemTesla's cars can achieve automated driving under specific conditions [57].

The research project on CAVs in China was led by Baidu DL institute in 2013. Following this, Baidu established the automotive networking business division in 2014 and launched several products such as CarLife, My-car, CoDriver, and more [204]. In 2016, a strategic signing ceremony was held between Baidu and Wuzhen Tourism to announce the implementation of unmanned driving at Level 4 in the scenic area. Other IT companies in China like Tencent, Alibaba, Huawei, etc. have also made significant progress in this field owing to their expertise in artificial intelligence [115]. For instance, Tencent collaborated with FAW (First Auto Work) to showcase the red flag Level 3 self-driving car.

VII. CONCLUSION

Smart vehicles are designed to provide a safer, more efficient, and more enjoyable driving experience for users. This paper presents a comprehensive survey and tutorial on smart vehicles, encompassing emerging technologies, security issues, and the implementation of machine learning and deep learning solutions. Firstly, we have explored the basic building blocks of smart vehicles, including electronic control units, in-vehicle networks, physical interfaces, wireless communication channels, sensors, and cameras. There are several ways in which attackers can exploit the attack surfaces in smart vehicles. Secondly, in security issues, we present common attack surfaces and types of security attacks that smart vehicles may face. In this paper, we have also explored the overall (non-security) challenges present in the automotive industry. Finally, we focused on the different methodologies, network technologies, and protocols categorically discussed in the literature and compiled a list of the security measures that have been implemented against the security threats on smart vehicles. We illustrated the role of the two most common techniques, i.e., machine learning and deep learning, in smart vehicle security.

ACKNOWLEDGMENT

The findings achieved herein are solely the authors' responsibility.

REFERENCES

[1] (2017). *Can Dataset for Intrusion Detection (OTIDS)*. Accessed: May 16, 2023. [Online]. Available: https://ocslab.hksecurity.net/Dataset/CAN-intrusion-dataset
[2] M. Abbott-Jard, H. Shah, and A. Bhaskar, "Empirical evaluation of Bluetooth and WiFi scanning for road transport," in *Proc. 36th Australas. Transp. Res. Forum (ATRF)*, vol. 14, 2013, pp. 1–14.
[3] A. F. Agarap, "Deep learning using rectified linear units (ReLU)," 2018, *arXiv:1803.08375*.
[4] U. Ahmad, "A node pairing approach to secure the Internet of Things using machine learning," *J. Comput. Sci.*, vol. 62, Jul. 2022, Art. no. 101718.

[5] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Secure passive keyless entry and start system using machine learning," in *Proc. 11th Int. Conf. Satell. Workshops Secur., Privacy, Anonymity Comput., Commun., Storage (SpaCCS)*. Melbourne, VIC, Australia: Springer, 2018, pp. 304–313.

[6] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Securing smart vehicles from relay attacks using machine learning," *J. Supercomput.*, vol. 76, no. 4, pp. 2665–2682, Apr. 2020.

[7] A. Ahmed, M. M. Iqbal, S. Jabbar, M. Ibrar, A. Erbad, and H. Song, "Position-based emergency message dissemination schemes in the Internet of Vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 13548–13572, Dec. 2023.

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

[9] K. M. Ali Alheeti, R. Al-Zaidi, J. Woods, and K. McDonald-Maier, "An intrusion detection scheme for driverless vehicles based gyroscope sensor profiling," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2017, pp. 448–449.

[10] K. M. Ali Alheeti and K. McDonald-Maier, "An intelligent intrusion detection scheme for self-driving vehicles based on magnetometer sensors," in *Proc. Int. Conf. Students Appl. Eng. (ICSAE)*, Oct. 2016, pp. 75–78.

[11] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "Intelligent intrusion detection of grey hole and rushing attacks in self-driving vehicular networks," *Computers*, vol. 5, no. 3, p. 16, 2016.

[12] M. Z. Alom et al., "The history began from AlexNet: A comprehensive survey on deep learning approaches," 2018, *arXiv:1803.01164*.

[13] A. Alshammari, M. A. Zohdy, D. Debnath, and G. Corser, "Classification approach for intrusion detection in vehicle systems," *Wireless Eng. Technol.*, vol. 9, no. 4, pp. 79–94, 2018.

[14] M. Amoozadeh et al., "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 126–132, Jun. 2015.

[15] I. M. Anjasmara et al., "Accuracy analysis of GNSS (GPS, GLONASS and BeiDou) obsevation for positioning," in *Proc. E3S Web Conf.*, vol. 94, 2019, p. 01019.

[16] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: A survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, May 2013.

[17] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, Oct. 2019, Art. no. 100179.

[18] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, "A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6206–6221, Jul. 2022.

[19] A. M. Aung, Y. Fadila, R. Gondokaryono, and L. Gonzalez, "Building robust deep neural networks for road sign detection," 2017, *arXiv:1712.09327*.

[20] D. Basavaraj and S. Tayeb, "Towards a lightweight intrusion detection framework for in-vehicle networks," *J. Sensor Actuator Netw.*, vol. 11, no. 1, p. 6, Jan. 2022.

[21] I. Berger, R. Rieke, M. Kolomeets, A. Chechulin, and I. Kotenko, "Comparative study of machine learning methods for in-vehicle intrusion detection," in *Proc. Comput. Secur., ESORICS Int. Workshops (CyberICPS SECPRE)*. Barcelona, Spain: Springer, Sep. 2019, pp. 85–101.

[22] S. Bharati, P. Podder, M. R. H. Mondal, and M. R. A. Robel, "Threats and countermeasures of cyber security in direct and remote vehicle communication systems," 2020, *arXiv:2006.08723*.

[23] B. Biggio, B. Nelson, and P. Laskov, "Poisoning attacks against support vector machines," 2012, *arXiv:1206.6389*.

[24] M. Birdsall, "Google and ITE: The road ahead for self-driving cars," *Inst. Transp. Eng. ITE J.*, vol. 84, no. 5, pp. 36–39, 2014.

[25] S. Bittl et al., "Emerging attacks on VANET security based on GPS time spoofing," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 344–352.

[26] J. J. Blum, A. Eskandarian, and L. J. Hoffman, "Challenges of intervehicle ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 5, no. 4, pp. 347–351, Dec. 2004.

[27] G. Bonaccorso, *Machine Learning Algorithms: Popular Algorithms for Data Science and Machine Learning*. Birmingham, U.K.: Packt, 2018.

[28] M. Borg et al., "Safely entering the deep: A review of verification and validation for machine learning and a challenge elicitation in the automotive industry," 2018, *arXiv:1812.05389*.

[29] A. Boukerche and E. Robson, "Vehicular cloud computing: Architectures, applications, and mobility," *Comput. Netw.*, vol. 135, pp. 171–189, Apr. 2018.

[30] A. K. Brown and M. A. Sturza, "Vehicle tracking system employing global positioning system (GPS) satellites," U.S. Patent 5 225 842, Jul. 6, 1993.

[31] O. Brun et al., "Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments," in *Proc. 1st Int. ISCIS Secur. Workshop Secur. Comput. Inf. Sci. (EuroCYBERSEC)*. London, U.K.: Springer, Feb. 2018, pp. 79–89.

[32] Z. Cai, A. Wang, W. Zhang, M. Gruffke, and H. Schweppe, "0-days & mitigations: Roadways to exploit and secure connected BMW cars," *Black Hat USA*, vol. 2019, p. 39, Aug. 2019.

[33] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald, "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions," in *Proc. 10th Annu. Cyber Inf. Secur. Res. Conf.*, 2015, pp. 1–8.

[34] R. Chai, D. Liu, T. Liu, A. Tsourdos, Y. Xia, and S. Chai, "Deep learning-based trajectory planning and control for autonomous ground vehicle parking maneuver," *IEEE Trans. Autom. Sci. Eng.*, vol. 20, pp. 1633–1647, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:250001248

[35] R. Chai, H. Niu, J. Carrasco, F. Arvin, H. Yin, and B. Lennox, "Design and experimental validation of deep reinforcement learning-based fast trajectory planning and control for mobile robot in unknown environment," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 35, no. 4, pp. 5778–5792, 2024, doi: 10.1109/TNNLS.2022.3209154.

[36] R. Chai, A. Tsourdos, S. Chai, Y. Xia, A. Savvaris, and C. L. P. Chen, "Multiphase overtaking maneuver planning for autonomous ground vehicles via a desensitized trajectory optimization approach," *IEEE Trans. Ind. Informat.*, vol. 19, no. 1, pp. 74–87, Jan. 2023.

[37] R. Chai, A. Tsourdos, H. Gao, S. Chai, and Y. Xia, "Attitude tracking control for reentry vehicles using centralised robust model predictive control," *Automatica*, vol. 145, Nov. 2022, Art. no. 110561.

[38] R. Chai, A. Tsourdos, H. Gao, Y. Xia, and S. Chai, "Dual-loop tube-based robust model predictive attitude tracking control for spacecraft with system constraints and additive disturbances," *IEEE Trans. Ind. Electron.*, vol. 69, no. 4, pp. 4022–4033, Apr. 2022.

[39] R. Chai, A. Tsourdos, A. Savvaris, S. Chai, Y. Xia, and C. L. P. Chen, "Design and implementation of deep neural network-based control for automatic parking maneuver process," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 4, pp. 1400–1413, Apr. 2022.

[40] R. N. Charette, "This car runs on code," IEEE Spectrum: Technol., Eng., Sci. News, 2009. Accessed: May 19, 2023. [Online]. Available: https://spectrum.ieee.org/this-car-runs-on-code

[41] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, vol. 4, San Francisco, CA, USA, 2011, p. 2021.

[42] L. Cheng, H.-M. Tsai, W. Viriyasitavat, and M. Boban, "Comparison of radio frequency and visible light propagation channel for vehicular communications," in *Proc. 1st ACM Int. Workshop Smart, Auto., Connected Veh. Syst. Services*, Oct. 2016, pp. 66–67.

[43] T. W. Chim, S.-M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.

[44] G. Clark, M. Doran, and W. Glisson, "A malicious attack on the machine learning policy of a robotic system," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng.*, Aug. 2018, pp. 516–521.

[45] L. M. Clements and K. M. Kockelman, "Economic effects of automated vehicles," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2606, no. 1, pp. 106–114, Jan. 2017.

[46] E Commission. *2016 Road Safety Statistics: What is Behind the Figures?* Accessed: May 26, 2023. [Online]. Available: https://europa.eu/rapid/press-release_MEMO-17-675_en.htm

[47] J. Cui and G. Sabaliauskaite, "US 2: An unified safety and security analysis method for autonomous vehicles," in *Proc. Future Inf. Commun. Conf. Adv. Inf. Commun. Netw. (FICC)*, vol. 1. London, U.K.: Springer, 2018, pp. 600–611.

[48] F. Cunha et al., "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Netw.*, vol. 44, pp. 90–103, Jul. 2016.

[49] E. S. da Silva, H. Pedrini, and A. Santos, "Applying graph neural networks to support decision making on collective intelligent transportation systems," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 4, pp. 4085–4096, Dec. 2023.

[50] R. M. Daoud, H. H. Amer, H. M. Elsayed, and Y. Sallez, "Ethernet-based car control network," in *Proc. Can. Conf. Electr. Comput. Eng.*, 2006, pp. 1031–1034.

[51] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "Prediction-based GNSS spoofing attack detection for autonomous vehicles," 2020, *arXiv:2010.11722*.

[52] J. DeCuir, "Introducing Bluetooth smart: Part 1: A look at both classic and new technologies," *IEEE Consum. Electron. Mag.*, vol. 3, no. 1, pp. 12–18, Jan. 2014.

[53] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "ImageNet: A large-scale hierarchical image database," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2009, pp. 248–255.

[54] N Developers. *NVIDIA Drive PX 2 Archive*. Accessed: May 26, 2023. [Online]. Available: https://developer.nvidia.com/drive/px2

[55] C. Diao, D. Zhang, W. Liang, K.-C. Li, Y. Hong, and J.-L. Gaudiot, "A novel spatial–temporal multi-scale alignment graph neural network security model for vehicles prediction," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 904–914, Jan. 2023.

[56] M. Dibaei et al., "An overview of attacks and defences on intelligent connected vehicles," 2019, *arXiv:1907.07455*.

[57] M. Dikmen and C. Burns, "Trust in autonomous vehicles: The case of tesla autopilot and summon," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, Oct. 2017, pp. 1093–1098.

[58] P. Dollár, C. Wojek, B. Schiele, and P. Perona, "Pedestrian detection: An evaluation of the state of the art," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 4, pp. 743–761, Apr. 2011.

[59] G. Dupont, A. Lekidis, J. Den Hartog, and S. Etalle, "Automotive controller area network (CAN) bus intrusion dataset v2," Centre Res. Data, Tech. Rep., 2019, doi: 10.4121/uuid:b74b4928-c377-4585-9432-2004dfa20a5d.

[60] T. Ebinuma. (2021). *Software-Defined GPS Signal Simulator, Github*. Accessed: May 26, 2023. [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[61] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016.

[62] CSS Electronics. *Can Bus Explained—A Simple Intro*. Accessed: Apr. 30, 2023. [Online]. Available: https://www.csselectronics.com/pages/can-bus-simple-intro-tutorial

[63] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses," *IEEE Access*, vol. 9, pp. 162401–162437, 2021.

[64] A. Eskandarian, *Handbook of Intelligent Vehicles*, vol. 2. London, U.K.: Springer, 2012.

[65] A. Ess, B. Leibe, K. Schindler, and L. Van Gool, "A mobile vision system for robust multi-person tracking," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2008, pp. 1–8.

[66] X. Feng, C.-Y. Li, D.-X. Chen, and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 2, pp. 305–314, Mar. 2017.

[67] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "Effective GPS jamming techniques for UAVs using low-cost SDR platforms," *Wireless Pers. Commun.*, vol. 115, no. 4, pp. 2705–2727, Dec. 2020.

[68] R. D. R. Fontes, C. Campolo, C. E. Rothenberg, and A. Molinaro, "From theory to experimental evaluation: Resource management in software-defined vehicular networks," *IEEE Access*, vol. 5, pp. 3069–3076, 2017.

[69] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.

[70] D. Gao et al., "A nationwide census on WiFi security threats: Prevalence, riskiness, and the economics," in *Proc. 27th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2021, pp. 242–255.

[71] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, "Congestion attacks to autonomous cars using vehicular botnets," in *Proc. NDSS Workshop Secur. Emerg. Netw. Technol. (SENT)*, San Diego, CA, USA, 2015, pp. 1–9.

[72] A. Geiger, P. Lenz, C. Stiller, and R. Urtasun, "Vision meets robotics: The KITTI dataset," *Int. J. Robot. Res.*, vol. 32, no. 11, pp. 1231–1237, 2013.

[73] A. Geiger, P. Lenz, and R. Urtasun, "Are we ready for autonomous driving? The KITTI vision benchmark suite," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2012, pp. 3354–3361.

[74] A. Ghosh et al., "Heterogeneous cellular networks: From theory to practice," *IEEE Commun. Mag.*, vol. 50, no. 6, pp. 54–64, Jun. 2012.

[75] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," 2014, *arXiv:1412.6572*.

[76] D. Gopinath, G. Katz, C. S. Pasareanu, and C. Barrett, "DeepSafe: A data-driven approach for checking adversarial robustness in neural networks," 2017, *arXiv:1710.00486*.

[77] N. A. Greenblatt, "Self-driving cars and the law," *IEEE Spectr.*, vol. 53, no. 2, pp. 46–51, Feb. 2016.

[78] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.

[79] M. A. Habib et al., "Security and privacy based access control model for Internet of Connected vehicles," *Future Gener. Comput. Syst.*, vol. 97, pp. 687–696, Aug. 2019.

[80] M. Han, P. Cheng, and S. Ma, "CVNNS-IDS: Complex-valued neural network based in-vehicle intrusion detection system," in *Proc. 1st Int. Conf. Secur. Privacy Digit. Economy (SPDE)*. Quzhou, China: Springer, Nov. 2020, pp. 263–277.

[81] M. Han, Z. Yin, P. Cheng, X. Zhang, and S. Ma, "Zero-knowledge identity authentication for Internet of Vehicles: Improvement and application," *PLoS ONE*, vol. 15, no. 9, Sep. 2020, Art. no. e0239043.

[82] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 2681–2691, 2015.

[83] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2016, pp. 770–778.

[84] J. Henriksson, M. Borg, and C. Englund, "Automotive safety and machine learning: Initial results from a study on how to adapt the ISO 26262 safety standard," in *Proc. 1st Int. Workshop Softw. Eng. AI Auto. Syst.*, 2018, pp. 47–49.

[85] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," 2015, *arXiv:1503.02531*.

[86] T. Hoppe and J. Dittman, "Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy," in *Proc. 2nd Workshop Embedded Syst. Secur. (WESS)*, 2007, pp. 1–6.

[87] S. Hoque, Md. Y. Arafat, S. Xu, A. Maiti, and Y. Wei, "A comprehensive review on 3D object detection and 6D pose estimation with deep learning," *IEEE Access*, vol. 9, pp. 143746–143770, 2021.

[88] J. Huang, M. Zhao, Y. Zhou, and C.-C. Xing, "In-vehicle networking: Protocols, challenges, and solutions," *IEEE Netw.*, vol. 33, no. 1, pp. 92–98, Jan. 2019.

[89] R. Huang, B. Xu, D. Schuurmans, and C. Szepesvári, "Learning with a strong adversary," 2015, *arXiv:1511.03034*.

[90] X. Huang et al., "The apolloscape dataset for autonomous driving," in *Proc. IEEE Conf. Computer Vis. Pattern Recognit. Workshops*, 2018, pp. 954–960.

[91] U Inc. (2018). *Udacity Self-Driving Car Dataset*. Accessed: May 26, 2023. [Online]. Available: https://www.kaggle.com/datasets/sshikamaru/udacity-self-driving-car-dataset

[92] I. Ivanov, C. Maple, T. Watson, and S. Lee, "Cyber security standards and issues in V2X communications for Internet of Vehicles," in *Proc. Living Internet Things, Cybersecurity (IoT)*, 2018, pp. 1–6.

[93] S. Jain, N. J. Ahuja, P. Srikanth, K. V. Bhadane, B. Nagaiah, A. Kumar, and C. Konstantinou, "Blockchain and autonomous vehicles: Recent advances and future directions," *IEEE Access*, vol. 9, pp. 130264–130328, 2021.

[94] K. Jaisingh, K. El-Khatib, and R. Akalu, "Paving the way for intelligent transport systems (ITS): Privacy implications of vehicle infotainment and telematics systems," in *Proc. 6th ACM Symp. Develop. Anal. Intell. Veh. Netw. Appl.*, Nov. 2016, pp. 25–31.

[95] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, "Caffe: Convolutional architecture for fast feature embedding," in *Proc. 22nd ACM Int. Conf. Multimedia*, Nov. 2014, pp. 675–678.

[96] H. J. Jo, W. Choi, S. Y. Na, S. Woo, and D. H. Lee, "Vulnerabilities of Android OS-based telematics system," *Wireless Pers. Commun.*, vol. 92, no. 4, pp. 1511–1530, 2017.

[97] N. Joubert, T. G. R. Reid, and F. Noble, "Developments in modern GNSS and its impact on autonomous vehicle architectures," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Oct. 2020, pp. 2029–2036.

[98] M. Jukl and J. Čupera, "Using of tiny encryption algorithm in CAN-bus communication," *Res. Agricult. Eng.*, vol. 62, no. 2, pp. 50–55, Jun. 2016.

[99] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, Jun. 2016, Art. no. e0155781.

[100] G. Karopoulos, G. Kambourakis, E. Chatzoglou, J. L. Hernández-Ramos, and V. Kouliaridis, "Demystifying in-vehicle intrusion detection systems: A survey of surveys and a meta-taxonomy," *Electronics*, vol. 11, no. 7, p. 1072, Mar. 2022.

[101] D. Kenjić, M. Antić, and M. Bjelica, "Evaluation of Ethernet subsystem for domain controller in autonomous vehicles," in *Proc. Zooming Innov. Consum. Technol. Conf. (ZINC)*, May 2021, pp. 59–63.

[102] K. Kiela et al., "Review of V2X–IoT standards and frameworks for ITS applications," *Appl. Sci.*, vol. 10, no. 12, p. 4314, Jun. 2020.

[103] P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in-vehicle network in the connected car," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2011, pp. 528–533.

[104] D. Klinedinst and C. King, "On board diagnostics: Risks and vulnerabilities of the connected vehicle," 2016. Accessed: Apr. 10, 2023. [Online]. Available: https://insights.sei.cmu.edu/blog/board-diagnostics-risks-and-vulnerabilities-connected-vehicle/

[105] M. Köhler et al., "Considerations for future automotive radar in the frequency range above 100 GHz," in *Proc. IEEE German Microw. Conf. (GeMIC)*, Mar. 2010, pp. 284–287.

[106] P. Koopman and M. Wagner, "Autonomous vehicle safety: An interdisciplinary challenge," *IEEE Intell. Transp. Syst. Mag.*, vol. 9, no. 1, pp. 90–96, Mar. 2017.

[107] K. Koscher et al., "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[108] A. Krizhevsky et al., "Learning multiple layers of features from tiny images," 2009. Accessed: May 15, 2023. [Online]. Available: https://www.cs.toronto.edu/kriz/learning-features-2009-TR.pdf

[109] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, May 2017.

[110] S. Kuutti, R. Bowden, Y. Jin, P. Barber, and S. Fallah, "A survey of deep learning applications to autonomous vehicle control," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 2, pp. 712–733, Feb. 2021.

[111] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[112] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.

[113] Y. Leng and L. Zhao, "Novel design of intelligent Internet-of-Vehicles management system based on cloud-computing and Internet-of-Things," in *Proc. Int. Conf. Electron. Mech. Eng. Inf. Technol.*, Aug. 2011, pp. 3190–3193.

[114] X. Li, Y. Yu, G. Sun, and K. Chen, "Connected vehicles' security from the perspective of the in-vehicle network," *IEEE Netw.*, vol. 32, no. 3, pp. 58–63, May 2018.

[115] Y. Li, J. Wang, T. Xing, T. Liu, C. Li, and K. Su, "TAD16K: An enhanced benchmark for autonomous driving," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2017, pp. 2344–2348.

[116] L. Liang, H. Ye, and G. Y. Li, "Toward intelligent vehicular networks: A machine learning framework," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 124–135, Feb. 2019.

[117] K. Lim, K. M. Tuladhar, and H. Kim, "Detecting location spoofing using ADAS sensors in VANETs," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2019, pp. 1–4.

[118] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: Timed efficient and secure vehicular communications with privacy preserving," *IEEE Trans. Wireless Commun.*, vol. 7, no. 12, pp. 4987–4998, Dec. 2008.

[119] H. L. Liu, J. S. Ma, S. Y. Zhu, Z. J. Lu, and Z. L. Liu, "Practical contactless attacks on Hitag2-based immobilizer and RKE systems," in *Proc. Int. Conf. Comput., Commun. Netw. Technol.*, 2018, pp. 505–512.

[120] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Netw.*, vol. 31, no. 5, pp. 50–58, Sep. 2017.

[121] S. Liu, L. Liu, J. Tang, B. Yu, Y. Wang, and W. Shi, "Edge computing for autonomous driving: Opportunities and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1697–1716, Aug. 2019.

[122] S. Liu, J. Tang, Z. Zhang, and J.-L. Gaudiot, "CAAD: Computer architecture for autonomous driving," 2017, *arXiv:1702.01894*.

[123] W LLC. (2019). *Waymo Open Dataset: An Autonomous Driving Dataset*.

[124] L. George, K. Eirini, P. Emmanouil, S. Panagiotis, B. Anatolij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Netw.*, vol. 84, pp. 124–147, Mar. 2019.

[125] J. J. Lu, T. Issaranon, and D. Forsyth, "SafetyNet: Detecting and rejecting adversarial examples robustly," in *Proc. IEEE Int. Conf. Comput. Vis.*, Oct. 2017, pp. 446–454.

[126] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "AI-based malicious network traffic detection in VANETs," *IEEE Netw.*, vol. 32, no. 6, pp. 15–21, Nov. 2018.

[127] W. Maddern, G. Pascoe, C. Linegar, and P. Newman, "1 year, 1000 km: The Oxford RobotCar dataset," *Int. J. Robot. Res.*, vol. 36, no. 1, pp. 3–15, Jan. 2017. [Online]. Available: https://robotcar-dataset.robots.ox.ac.uk/images/robotcar_ijrr.pdf

[128] K. R. Malik, M. Ahmad, S. Khalid, H. Ahmad, F. Al-Turjman, and S. Jabbar, "Image and command hybrid model for vehicle control using Internet of Vehicles," *Trans. Emerg. Telecommun. Technol.*, vol. 31, no. 5, p. e3774, May 2020.

[129] X. Mao, D. Inoue, H. Matsubara, and M. Kagami, "Demonstration of in-car Doppler laser radar at 1.55 μm for range and speed measurement," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 2, pp. 599–607, Jun. 2013.

[130] S. Mazloom, M. Rezaeirad, A. Hunter, and D. McCoy, "A security analysis of an in-vehicle infotainment and app platform," in *Proc. WOOT*, 2016, pp. 232–243.

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

[132] A. Miglani and N. Kumar, "Deep learning models for traffic flow prediction in autonomous vehicles: A review, solutions, and challenges," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100184.

[133] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *Def. Con.*, vol. 21, nos. 260–264, pp. 15–31, 2013.

[134] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, no. S91, pp. 1–91, Aug. 2015.

[135] Mobileye. *Eyeq® the System-on-Chip for Automotive Applications*. Accessed: May 26, 2023.

[136] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Eng. J.*, vol. 54, no. 4, pp. 1115–1126, Dec. 2015.

[137] U. Montanaro et al., "Towards connected autonomous driving: Review of use-cases," *Veh. Syst. Dyn.*, vol. 57, no. 6, pp. 779–814, 2019.

[138] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, Apr. 2018.

[139] O. Nakhila, E. Dondyk, M. F. Amjad, and C. Zou, "User-side Wi-Fi evil twin attack detection using SSL/TCP protocols," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2015, pp. 239–244.

[140] S. N. Narayanan, S. Mittal, and A. Joshi, "Using data analytics to detect anomalous states in vehicles," 2015, *arXiv:1512.08048*.

[141] S. N. Narayanan, S. Mittal, and A. Joshi, "OBD_SecureAlert: An anomaly detection system for vehicles," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, 2016, pp. 1–6.

[142] S. Narbayeva, T. Bakibayev, K. Abeshev, I. Makarova, K. Shubenkova, and A. Pashkevich, "Blockchain technology on the way of autonomous vehicles development," *Transp. Res. Proc.*, vol. 44, pp. 168–175, Jan. 2020.

[143] A. J. Neumann, N. Statland, and R. D. Webb, "Post-processing audit tools and techniques," in *Proc. Invitational Workshop (NBS)*, Miami Beach, FL, USA: U.S. Department of Commerce, National Bureau of Standards, 1977, pp. 3–11.

[144] NHTSA. (2016). *Fatal Motor Vehicle Crashes: Overview*. Accessed: May 26, 2023.

[145] S. Nie, L. Liu, and Y. Du, "Free-fall: Hacking tesla from wireless to CAN bus," *Briefing Black Hat USA*, vol. 25, pp. 1–16, Jul. 2017.

[146] D. K. Nilsson and U. E. Larson, "Simulated attacks on can buses: Vehicle virus," in *Proc. IASTED Int. Conf. Commun. Syst. Netw. (AsiaCSN)*, 2008, pp. 66–72.

[147] D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient in-vehicle delayed data authentication based on compound message authentication codes," in *Proc. IEEE 68th Veh. Technol. Conf.*, Sep. 2008, pp. 1–5.

[148] NIST. (2017). *Guide to LTE Security*. Accessed: May 15, 2023.

[149] OECD. (2021). *Road Accidents (Indicator)*. Accessed: Jun. 2, 2023. [Online]. Available: https://data.oecd.org/transport/road-accidents.htm

[150] L. P. O. Lange. (2020). *Traffic Prediction With Advanced Graph Neural Networks*. Accessed: May 26, 2023. [Online]. Available: https://deepmind.google/discover/blog/traffic-prediction-with-advanced-graph-neural-networks/

[151] World Health Organization. (2018). *Global Status Report on Road Safety*. Accessed: May 26, 2023. [Online]. Available: https://www.who.int/publications/i/item/9789241565684

[152] N. Papernot, P. McDaniel, X. Wu, S. Jha, and A. Swami, "Distillation as a defense to adversarial perturbations against deep neural networks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2016, pp. 582–597.

[153] K. Pazul, "Controller area network (CAN) basics," Microchip Technol. Inc., Tech. Rep. DS00713A, vol. 1, 1999.

[154] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2014. [Online]. Available: https://www.semanticscholar.org/paper/Potential-Cyberattacks-on-Automated-Vehicles-Petit-Shladover/b9e44002a56f398708179f95f7de5deb24c6ead8

[155] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," *Black Hat Europe*, vol. 11, no. 2015, p. 995, 2015. [Online]. Available: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf

[156] S. G. Philipsen, B. Andersen, and B. Singh, "Threats and attacks to modern vehicles," in *Proc. IEEE Int. Conf. Internet Things Intell. Syst. (IoTaIS)*, Nov. 2021, pp. 22–27.

[157] A. Protogerou, S. Papadopoulos, A. Drosou, D. Tzovaras, and I. Refanidis, "A graph neural network method for distributed anomaly detection in IoT," *Evolving Syst.*, vol. 12, no. 1, pp. 19–36, Mar. 2021.

[158] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[159] L. L. Pullum, B. J. Taylor, and M. A. Darrah, *Guidance for the Verification and Validation of Neural Networks*, vol. 11. Hoboken, NJ, USA: Wiley, 2007.

[160] A. Qayyum, M. Usama, J. Qadir, and A. Al-Fuqaha, "Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 998–1026, 2nd Quart., 2020.

[161] V. Rajaraman, "Johnmccarthy—Father of artificial intelligence," *Resonance*, vol. 19, pp. 198–207, Mar. 2014.

[162] G. K. Rajbahadur, A. J. Malton, A. Walenstein, and A. E. Hassan, "A survey of anomaly detection for connected vehicle cybersecurity and safety," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 421–426.

[163] M. Rasib et al., "Are self-driving vehicles ready to launch? An insight into steering control in autonomous self-driving vehicles," *Math. Problems Eng.*, vol. 2021, pp. 1–22, Feb. 2021.

[164] M. S. Rathore et al., "A novel trust-based security and privacy model for Internet of Vehicles using encryption and steganography," *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108205.

[165] V. Rausch, A. Hansen, E. Solowjow, C. Liu, E. Kreuzer, and J. K. Hedrick, "Learning a deep neural net policy for end-to-end control of autonomous vehicles," in *Proc. Amer. Control Conf. (ACC)*, 2017, pp. 4914–4919.

[166] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, 2007.

[167] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux, "Certificate revocation in vehicular networks," Lab. Comput. Commun. Appl. (LCA), School Comput. Commun. Sci., EPFL, Switzerland, Tech. Rep., 2006, pp. 1–10.

[168] S. Raza, S. Wang, M. Ahmed, and M. R. Anwar, "A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–19, Feb. 2019.

[169] J. Ren, H. Gaber, and S. S. Al Jabar, "Applying deep learning to autonomous vehicles: A survey," in *Proc. 4th Int. Conf. Artif. Intell. Big Data (ICAIBD)*, May 2021, pp. 247–252.

[170] B Report. (2018). *Volkswagen and Audi Cars Vulnerable to Remote Hacking*. Accessed: May 20, 2023.

[171] (2016). *L Report*.

[172] F. Riaz, S. Jabbar, M. Sajid, M. Ahmad, K. Naseer, and N. Ali, "A collision avoidance scheme for autonomous vehicles inspired by human social norms," *Comput. Electr. Eng.*, vol. 69, pp. 690–704, Jul. 2018.

[173] I. Rouf et al., "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. USENIX Secur. Symp.*, vol. 10, 2010, p. 21.

[174] Z. G. Ruthberg and R. G. McKenzie, "Audit and evaluation of computer security," Tech. Rep., 1977.

[175] R. Sagar, "Making cars safer through technology innovation," Texas Instrum., Dallas, TX, USA, Tech. Rep., 2017, pp. 1–10. [Online]. Available: https://www.ti.com/lit/wp/sszy009a/sszy009a.pdf?ts=1720169668258&ref_url=https%253A%252F%252Fwww.ti.com.cn%252Fdocument-viewer%252Fcn%252Flit%252Fhtml%%252FGUID-88788D10-992D-4DAD-BB28-605C32A2A7C9

[176] R. Salay, R. Queiroz, and K. Czarnecki, "An analysis of ISO 26262: Using machine learning safely in automotive software," 2017, *arXiv:1709.02435*.

[177] F. M. Salem, M. H. Ibrahim, and I. I. Ibrahim, "Non-interactive authentication scheme providing privacy among drivers in vehicle-to-vehicle networks," in *Proc. 6th Int. Conf. Netw. Services*, Mar. 2010, pp. 156–161.

[178] G. Samara and Y. Al-Raba'nah, "Security issues in vehicular ad hoc networks (VANET): A survey," 2017, *arXiv:1712.04263*.

[179] R. Sattiraju, D. Wang, A. Weinand, and H. D. Schotten, "Link level performance comparison of C-V2X and ITS-G5 for vehicular channel models," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–7.

[180] A. Sawant, S. Lenina, and D. Joshi, "CAN, FlexRay, MOST versus Ethernet for vehicular networks," *Int. J. Innov. Advancement Comput. Sci.*, vol. 7, no. 4, pp. 1–4, 2018.

[181] S. E. Shladover, C. Nowakowski, X.-Y. Lu, and R. Ferlis, "Cooperative adaptive cruise control: Definitions and operating concepts," *Transp. Res. Rec.*, vol. 2489, no. 1, pp. 145–152, Jan. 2015.

[182] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Proc. 15th Int. Workshop Cryptograph. Hardw. Embedded Syst. (CHES)*. Santa Barbara, CA, USA: Springer, Aug. 2013, pp. 55–72.

[183] S. Shreejith et al., "VEGa: A high performance vehicular Ethernet gateway on hybrid FPGA," *IEEE Trans. Comput.*, vol. 66, no. 10, pp. 1790–1803, Oct. 2017.

[184] D. Shukla, A. Vaibhav, S. Das, and P. Johri, "Security and attack analysis for vehicular ad hoc network—A survey," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, 2016, pp. 625–630.

[185] F. Siddiqui. *The University of Leuven Research Report, 202*. Accessed: May 15, 2023.

[186] A. X. A. Sim and B. Sitohang, "OBD-II standard car engine diagnostic software development," in *Proc. Int. Conf. Data Softw. Eng. (ICODSE)*, Nov. 2014, pp. 1–5.

[187] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, *arXiv:1409.1556*.

[188] S. Singh, "Critical reasons for crashes investigated in the national motor vehicle crash causation survey," Tech. Rep., 2015.

[189] C. Sitawarin, A. Nitin Bhagoji, A. Mosenia, M. Chiang, and P. Mittal, "DARTS: Deceiving autonomous cars with toxic signs," 2018, *arXiv:1802.06430*.

[190] C. Sitawarin, A. N. Bhagoji, A. Mosenia, P. Mittal, and M. Chiang, "Rogue signs: Deceiving traffic sign recognition with malicious ads and logos," 2018, *arXiv:1801.02780*.

[191] S. C. Stubberud and K. A. Kramer, "Threat assessment for GPS navigation," in *Proc. IEEE Int. Symp. Innov. Intell. Syst. Appl. (INISTA)*, Jun. 2014, pp. 287–292.

[192] C. Sulzberger, "An early road warrior: Electric vehicles in the early years of the automobile," *IEEE Power Energy Mag.*, vol. 2, no. 3, pp. 66–71, May 2004.

[193] I. A. Sumra, H. B. Hasbullah, and J.-L. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," in *Proc. 1st Int. Workshop Veh. Ad-Hoc Netw. Smart Cities*. Singapore: Springer, 2014, pp. 51–61.

[194] J. Sun, S. Iqbal, N. Seifollahpour Arabi, and M. Zulkernine, "A classification of attacks to in-vehicle components (IVCs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100253.

[195] C. Szegedy et al., "Going deeper with convolutions," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2015, pp. 1–9.

[196] S. C. Talbot and S. Ren, "Comparision of FieldBus systems CAN, TTCAN, FlexRay and LIN in passenger vehicles," in *Proc. 29th IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2009, pp. 26–31.

[197] M. Taraba, J. Adamec, M. Danko, and P. Drgona, "Utilization of modern sensors in autonomous vehicles," in *Proc. ELEKTRO*, 2018, pp. 1–5.

[198] A. Taylor, S. Leblanc, and N. Japkowicz, "Anomaly detection in automobile control network data with long short-term memory networks," in *Proc. IEEE Int. Conf. Data Sci. Adv. Anal. (DSAA)*, Oct. 2016, pp. 130–139.

[199] B. J. Taylor, *Methods and Procedures for the Verification and Validation of Artificial Neural Networks*. Hohhot, China: Springer, 2006.

[200] A. Theissler, "Anomaly detection in recordings from in-vehicle networks," *Big Data Appl.*, vol. 23, p. 26, Sep. 2014.
[201] V. L. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Dec. 2016, pp. 164–170.
[202] M. Thomas et al., *Global Navigation Space Systems: Reliance and Vulnerabilities*. London, U.K.: The Royal Academy of Engineering, 2011.
[203] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Secur.*, Oct. 2011, pp. 75–86.
[204] A. Toschi, M. Sanic, J. Leng, Q. Chen, C. Wang, and M. Guo, "Characterizing perception module performance and robustness in production-scale autonomous driving system," in *Proc. 16th IFIP WG 10.3 Int. Conf. Netw. Parallel Computing (NPC)*. Hohhot, China: Springer, Aug. 2019, pp. 235–247.
[205] S. Ucar, S. C. Ergen, and O. Ozkasap, "Data-driven abnormal behavior detection for autonomous platoon," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 69–72.
[206] A. Upadhyay, J. O. Ayodele, A. Kumar, and J. A. Garza-Reyes, "A review of challenges and opportunities of blockchain adoption for operational excellence in the U.K. automotive industry," *J. Global Operations Strategic Sourcing*, vol. 14, no. 1, pp. 7–60, Jul. 2021.
[207] M. Vanhoef and F. Piessens, "Denial of service attacks against the 4-way Wi-Fi handshake," in *Proc. Comput. Sci. Inf. Technol. (CS IT)*. Academy & Industry Research Collaboration Center (AIRCC), Nov. 2017, pp. 1–10.
[208] S. Wang and Y. He, "A trust system for detecting selective forwarding attacks in VANETs," in *Proc. 2nd Int. Conf. Big Data Comput. Communications (BigCom)*. Shenyang, China: Springer, 2016, pp. 377–386.
[209] Y. Wang, D. Zhang, Y. Liu, B. Dai, and L. H. Lee, "Enhancing transportation systems via deep learning: A survey," *Transp. Res. C, Emerg. Technol.*, vol. 99, pp. 144–163, Feb. 2019.
[210] J. S. Weber, M. Neves, and T. Ferreto, "VANET simulators: An updated review," *J. Braz. Comput. Soc.*, vol. 27, no. 1, pp. 1–31, 2021.
[211] W. Whyte, J. Petit, V. Kumar, J. Moring, and R. Roy, "Threat and countermeasures analysis for WAVE service advertisement," in *Proc. IEEE 18th Int. Conf. Intell. Transp. Syst.*, Sep. 2015, pp. 1061–1068.
[212] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Proc. Workshop Embedded Secur. Cars*, Bochum, Germany, 2004, pp. 1–13.
[213] S. Woo, H. J. Jo, and D. H. Lee, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.
[214] W. Wu et al., "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020.
[215] X. Wu et al., "Vehicular communications using DSRC: Challenges, enhancements, and evolution," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 399–408, Sep. 2013.
[216] F. Xu, H. Uszkoreit, Y. Du, W. Fan, D. Zhao, and J. Zhu, "Explainable AI: A brief survey on history, research areas, approaches and challenges," in *Proc. 8th CCF Int. Conf. Natural Lang. Process. Chin. Comput. (NLPCC)*. Dunhuang, China: Springer, Oct. 2019, pp. 563–574.
[217] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *Defcon*, vol. 24, no. 8, p. 109, 2016.
[218] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, "A novel data fusion algorithm to combat false data injection attacks in networked radar systems," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 4, no. 1, pp. 125–136, Mar. 2018.
[219] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 2, pp. 1–19, 2019.
[220] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proc. 1st Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services (MOBIQUITOUS)*, 2004, pp. 114–123.
[221] Y. Yao et al., "Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 591–602.
[222] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 1, p. 39, 2018.
[223] H. Ye and G. Y. Li, "Deep reinforcement learning for resource allocation in V2V communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[224] H. Ye, L. Liang, G. Y. Li, J. Kim, L. Lu, and M. Wu, "Machine learning for vehicular networks: Recent advances and application examples," *IEEE Veh. Technol. Mag.*, vol. 13, no. 2, pp. 94–101, Jun. 2018.
[225] H. Yin and C. Berger, "When to use what data set for your self-driving car algorithm: An overview of publicly available driving datasets," in *Proc. IEEE 20th Int. Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2017, pp. 1–8.
[226] Q. Yin, R. Zhang, and X. Shao, "CNN and RNN mixed model for image classification," in *Proc. MATEC Web Conf.*, vol. 277, 2019, p. 02001.
[227] X. Yuan, P. He, Q. Zhu, and X. Li, "Adversarial examples: Attacks and defenses for deep learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 9, pp. 2805–2824, Sep. 2019.
[228] S. Zeadally, J. Guerrero, and J. Contreras, "A tutorial survey on vehicle-to-vehicle communications," *Telecommun. Syst.*, vol. 73, no. 3, pp. 469–489, Mar. 2020.
[229] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012.
[230] N. Zhumadil, S. Narbayeva, T. Bakibayev, K. Abeshev, and K. Shubenkova, "Blockchain for vehicles based on exonum platform," *Synchroinfo J.*, vol. 7, pp. 24–29, 2021.

Usman Ahmad received the Ph.D. degree from Beijing Institute of Technology, China, in 2022. He is currently a Post-Doctoral Researcher with Jiangsu University, China, while holding the position of an Assistant Professor with The University of Faisalabad, Pakistan, currently on leave. His research interests include autonomous vehicles, cybersecurity, the IoT, machine learning, and artificial neural networks.

Mu Han (Member, IEEE) received the Ph.D. degree from the School of Computer Science and Technology, Nanjing University of Science and Technology, China, in 2011. She is currently a Professor with the School of Computer Science and Communication Engineering, Jiangsu University. Her research interests include cryptography, security, and communication in-vehicle networks, the design of security protocols for smart cars, and information security.

Alireza Jolfaei (Senior Member, IEEE) is currently an Associate Professor in cybersecurity and networking with the College of Science and Engineering, Flinders University. He is also a Distinguished Speaker of the ACM on the topic of cybersecurity. His main research interests are cyber-physical systems security, where he investigates the hidden interdependencies in industrial communication protocols and aims to provide fundamentally new methods for security-aware modeling, analysis, and design of safety-critical cyber-physical systems in the presence of cyber adversaries.

Mr. Jolfaei was the Founder and Councilor of the IEEE Student Branch at Federation University and also contributed to the foundation of the IEEE Northern Territory Subsection. He is a Distinguished Speaker of the ACM on the topic of Cybersecurity. He is the Chair of the Security and Privacy Technical Committee of the IEEE Consumer Technology Society. He has served as the IEEE Australia Chair for the IEEE Technology and Engineering Management Society for Membership Development and Activities, as the Secretary for the IEEE NSW Joint Chapter on Consumer Technology, Broadcast Technology, and Product Safety Engineering, and as the Chairperson of the Computational Intelligence Society for the IEEE Victoria Section, and the Professional and Career Activities for the IEEE Queensland Section. He is the Editor-in-Chief of the IEEE Consumer Technology Society's World Newsletter. He has served as an Associate Editor for several IEEE journals and transactions, including IEEE TRANSACTIONS ON CONSUMER TECHNOLOGY and IEEE INTERNET OF THINGS JOURNAL. He has served as the Program Co-Chair and a Technical Program Committee Member for major conferences, including IEEE ICCCN.

Sohail Jabbar is currently an Associate Professor with the College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia. Previously, he was a Professor with the Department of Computational Sciences, the Associate Dean (Faculty of IT), and the Director of ORIC with The University of Faisalabad, Faisalabad, Pakistan. He was also with the CfACS IoT Laboratory, Manchester Metropolitan University, U.K., as a Research Associate, in 2020, and a Post-Doctoral Fellow with the Network Laboratory, Kyungpook National University, Daegu, South Korea, in 2017. He has authored four book chapters and published over 100 research articles in prestigious journals. He was engaged in many national and international-level projects. He is a guest editor of special issues and an associate editor in leading journals of his domain. He is on collaborative research with renowned research centers and institutes worldwide on various topics in the IoT, WSN, and blockchain fields.

Muhammad Ibrar received the B.S. degree in telecommunication and networking from COMSATS University Islamabad, Abbottabad Campus, Pakistan, in 2010, the M.S. degree in telecommunication and networking from Bahria University, Islamabad, Pakistan, in 2014, and the Ph.D. degree from the School of Software, Dalian University of Technology, China, in 2021. He is currently a Post-Doctoral Researcher with the College of Science and Engineering, Hamad Bin Khalifa University, Qatar. His research interests include software-defined networking (SDN), fog computing, wireless ad-hoc, and sensor networks.

Aiman Erbad (Senior Member, IEEE) received the M.Sc. degree from the University of Essex, U.K., in 2005, and the Ph.D. degree from The University of British Columbia, Canada, in 2012. He is currently a Full Professor and the VP for Research and Graduate Studies at Qatar University. He has published more than 200 papers in top conferences and journals and helped organize many international IEEE and ACM conferences. His research interests include cloud computing, edge computing, the IoT, distributed AI, private/secure networks, and multimedia systems. He received the Platinum Award from the H. H. Emir Sheikh Tamim Bin Hamad Al Thani at the Education Excellence Day 2013 (Ph.D. category). He received four international best paper awards and more than 12 major research grants from Qatar National Research Fund programs. He is an editorial board member in four international journals.

Houbing Herbert Song (Fellow, IEEE) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in August 2012.

He is currently a Professor, the Director of the NSF Center for Aviation Big Data Analytics (Planning), the Associate Director for Leadership of the DOT Transportation Cybersecurity Center for Advanced Research and Education (Tier 1 Center), and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us), University of Maryland, Baltimore County (UMBC), Baltimore, MD, USA. He is also a Distinguished Visiting Fellow of the Scottish Informatics and Computer Science Alliance (SICSA). Prior to joining UMBC, he was a Tenured Associate Professor of electrical engineering and computer science with Embry–Riddle Aeronautical University, Daytona Beach, FL, USA. His research has been sponsored by federal agencies, including the National Science Foundation, the National Aeronautics and Space Administration, U.S. Department of Transportation, and the Federal Aviation Administration, and among others industry. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, IEEE Transmitter, inside BIGDATA, Association for Uncrewed Vehicle Systems International (AUVSI), Security Magazine, CXOTech Magazine, Fox News, U.S. News & World Report, The Washington Times, and New Atlas. He is the editor of ten books, the author of more than 100 articles, and the inventor of two patents. His research interests include AI/machine learning/big data analytics, cyber-physical systems/Internet of Things, and cybersecurity and privacy.

Dr. Song is an Asia-Pacific Artificial Intelligence Association (AAIA) Fellow, an ACM Distinguished Member, and a Full Member of Sigma Xi. He received the Research.com Rising Star of Science Award in 2022, the 2021 Harry Rowe Mimno Award bestowed by the IEEE Aerospace and Electronic Systems Society, and more than ten best paper awards from major international conferences, including IEEE CPSCom-2019, IEEE ICII 2019, IEEE/AIAA ICNS 2019, IEEE CBDCom 2020, WASA 2020, AIAA/IEEE DASC 2021, IEEE GLOBECOM 2021, and IEEE INFOCOM 2022. He has been serving as an Associate Editor for IEEE TRANSACTIONS ON ARTIFICIAL INTELLIGENCE since 2023, IEEE INTERNET OF THINGS JOURNAL since 2020, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS since 2021, and IEEE JOURNAL ON MINIATURIZATION FOR AIR AND SPACE SYSTEMS since 2020. He was an Associate Technical Editor of *IEEE Communications Magazine* from 2017 to 2020. He has been a Highly Cited Researcher identified by Web of Science since 2021. He has been an ACM Distinguished Speaker since 2020, an IEEE Computer Society Distinguished Visitor since 2024, an IEEE Communications Society (ComSoc) Distinguished Lecturer since 2024, an IEEE Intelligent Transportation Systems Society (ITSS) Distinguished Lecturer since 2024, an IEEE Vehicular Technology Society (VTS) Distinguished Lecturer since 2023, and an IEEE Systems Council Distinguished Lecturer since 2023. He has been an IEEE Impact Creator since 2023.

Yazeed Alkhrijah (Member, IEEE) received the B.S. degree in electrical engineering (communication and electronics) from King Saud University, Riyadh, Saudi Arabia, the M.S. degree in electrical and computer engineering from The University of Tennessee Knoxville, TN, USA, and the Ph.D. degree in electrical and computer engineering from Southern Methodist University, Dallas, TX, USA. In 2022, he joined as the Director of the Engineering Research Center and an Assistant Professor with Imam Muhammad Ibn Saud Islamic University, Riyadh.