IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 27, 2020, accepted November 8, 2020, date of publication November 16, 2020,
date of current version November 27, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3037705*

# Attacks on Self-Driving Cars and Their Countermeasures: A Survey

**ABDULLAHI CHOWDHURY[1], (Member, IEEE), GOUR KARMAKAR[1], (Member, IEEE), JOARDER KAMRUZZAMAN[1], (Senior Member, IEEE), ALIREZA JOLFAEI[2], (Senior Member, IEEE), AND RAJKUMAR DAS[3]**

[1]School of Engineering, IT and Physical Sciences, Federation University Australia, Ballarat, VIC 3350, Australia
[2]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
[3]Information Technology Service, Federation University Australia, Ballarat, VIC 3350, Australia

Corresponding author: Joarder Kamruzzaman (joarder.kamruzzaman@federation.edu.au)

**ABSTRACT** Intelligent Traffic Systems (ITS) are currently evolving in the form of a cooperative ITS or connected vehicles. Both forms use the data communications between Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I/I2V) and other on-road entities, and are accelerating the adoption of self-driving cars. The development of cyber-physical systems containing advanced sensors, sub-systems, and smart driving assistance applications over the past decade is equipping unmanned aerial and road vehicles with autonomous decision-making capabilities. The level of autonomy depends upon the make-up and degree of sensor sophistication and the vehicle's operational applications. As a result, self-driving cars are being compromised perceived as a serious threat. Therefore, analyzing the threats and attacks on self-driving cars and ITSs, and their corresponding countermeasures to reduce those threats and attacks are needed. For this reason, some survey papers compiling potential attacks on VANETs, ITSs and self-driving cars, and their detection mechanisms are available in the current literature. However, up to our knowledge, they have not covered the real attacks already happened in self-driving cars. To bridge this research gap, in this paper, we analyze the attacks that already targeted self-driving cars and extensively present potential cyber-attacks and their impacts on those cars along with their vulnerabilities. For recently reported attacks, we describe the possible mitigation strategies taken by the manufacturers and governments. This survey includes recent works on how a self-driving car can ensure resilient operation even under ongoing cyber-attack. We also provide further research directions to improve the security issues associated with self-driving cars.

**INDEX TERMS** Self-driving cars, intelligent transportation system, security attacks, mitigation strategies, cybersecurity, VANET.

## ACRONYMS

| | |
|---|---|
| **ACC** | Adaptive Cruise Control |
| **ADAS** | Advanced Driver Assistance Systems |
| **ATCSs** | Adaptive Traffic Control Systems |
| **ATS** | Adaptive Traffic Signal |
| **AU** | Application Unit |
| **AV** | Autonomous Vehicles |
| **CACC** | Cooperative Adaptive Cruise Control |
| **CAV** | Connected Autonomous Vehicle |
| **DoS** | Denial of Service |
| **DDoS** | Distributed Denial of Service |
| **ECU** | Electronic Control Unit |
| **EDCF** | Enhanced Distributed Coordination Function |
| **I2X** | Infrastructure to Everything |
| **GPS** | Global Positioning System |
| **GSM** | Global System for Mobile communication |
| **GNSS** | Global Navigation Satellite System |
| **I2I** | Infrastructure- to-Infrastructure |
| **IMS** | Incident Management System |
| **ITS** | Intelligent Traffic Systems |
| **IVWS** | Intersection Violation Warning System |
| **Lidar** | Light Detection and Ranging |
| **MANET** | Mobile ad hoc networks |
| **OBU** | Onboard Unit |
| **OFDM** | Orthogonal Frequency Division Multiplexing |

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

| | |
|---|---|
| **PMA** | Parking Management Application |
| **Radar** | Radio Detecting And Ranging |
| **RFID** | Radio Frequency Identification |
| **RSU** | Road Side Unit |
| **SC** | Self-driving Cars |
| **SDT** | Self-Driving Transport |
| **SGC** | Signal Controller |
| **TMS** | Traffic Management System |
| **TSP** | Trusted Service Providers |
| **TTP** | Trusted third parties |
| **V2I** | Vehicle-to-Infrastructure |
| **V2V** | Vehicle-to-Vehicle |
| **V2X** | Vehicle to Everything |
| **VANET** | Vehicular ad hoc network |
| **WAVE** | Wireless Access in Vehicular Environments |
| **WSN** | Wireless Sensor Network |

## I. INTRODUCTION

Self-driving cars are regarded as the next revolutionary technological advancement in the transport sector globally. They are anticipated to revolute global safety, especially when it comes to transportation efficiency, reduced congestion, minimum accidents, and other positive impacts. When the Intelligent Traffic Systems (ITS) developments gave this anticipated advancement to the world, many viewed it from the Autonomous Vehicle's (AV's) direction. Note that AVs include self-driving vehicles as well, and in the context of this paper, we use them interchangeably. The improvement has been an anticipated transport sector revolution, and it's kicking off soon from the way technology has been advancing over the past years. This will soon be like a dream that has come true to many people globally or a reality that was not expected to hit the world hard. Many Connected Autonomous Vehicles (CAVs) have integrated the various technological advancements to make the self-driving cars become a reality, which will offer improved efficiency as well as safe means of transport [1]. Through automatic data sharing, technical support of vehicle communication and the infrastructure will make this one of the best and widely considered means of transportation. These aspects that will be enabled through the technical advancements in traffic lines will allow better performance of the transport sector. From efficiency to high degrees of effectiveness, self-driving cars will be a win-win situation for the globe at large. Replacing human operations with technology has been giving the best results since the evolution of robotics and all machines that enhance automatic functions. In the same way, these cars will be automated and apply the sensor technology to improve efficiency in transport and fleet management [2].

The growth, as well as the viable publication of CAVs, has been mainly motivated by the global need of people to create an infrastructure that has fast and reliable safe means of commuting. The evolution of CAVs certainly needs a proliferation in high-tech assets. The self-driving carriages are fitted out with many antennas, including cameras, Radio Detecting And Ranging (Radar), and other replacements of manual mirrors of the current cars, which will enable them to maneuver on their own. This will be such a relief to drivers because the cars will be automatically controlled hence no need to hoot in jams and balance gears when stuck in traffic. This will be a stress relief to them from the tiresome long driving hours every day. Public road driving will be safer for both pedestrians and motorists because all cruise controls are automatically controlled as well as the brake pedals and all car control features [3]. With the improved features that enable automatic parking [4] in the yellow curbs or parking zones as well as the Advanced Driver Assistance Systems (ADASs) and controlled driving [5], there will be safe transportation. The efficiency that comes with these vehicles includes energy and natural resource preservation [5]. With a combination of all these positive features, these vehicles are a transformation that will have a positive impact on the world's transport sectors [6].

A fully automated vehicle depends on the sensor readings to make short-term (e.g., safety-related) and long-term (e.g., planning) driving decisions. Communication between the sensors is enhanced through the hi-tech infrastructure of these cars. The control panels of self-driving cars are advanced to enhance their autonomous movement. However, the technology world comes with risks and threats, especially the attacks from viruses, bugs, and hackers can be malicious. This is why self-driving cars have advanced data encryption and protection to enhance their reliability, accuracy, and other aspects. Automatic vehicles are integrated with many advanced systems that increase navigation abilities through road maps and radio frequency properties. Nevertheless, automatic vehicles still pose high risks of being exposed to threats, and attacks can be possible to occur on all technology devices fitted in them [7], [8].

Automatic vehicles have been developed in many models, and some successful models include standard Shelley, Google driverless cars, and the AnnieWAY [9]. These models have an object detection sensor and camera that recognize traffic lights. These cars generally have a good influence on planning the mission of self-driving vehicles launch. The sensors, such as Light Detection and Ranging (Lidar), have a view that detects obstacles on the road, and they can drive past such obstacles safely. That is how well the automatic cars are automated. They also have vital risks to fatal accidents occurring, especially when a malicious attack occurs due to hacking or virus attacks. In case a sensor is attacked by hackers and the data readability gets messed up, an accident can occur. They are safe as long as the data is not affected or degraded in any way that can alter their accuracy. Currently, these automatic vehicles are under development stages, and they will be available in the market soon. They need thorough phases of manufacturing, incorporation of all automated features to ensure there is no risk of malicious attacks, including cyber-attacks [9]. Law makers of different countries (e.g., USA, Australia, China, Singapore, South Korea) [10]–[18]

have implemented or are implementing different governing strategies to increase the security and privacy of the data used and transmitted by the autonomous vehicles.

The concerns about security issues have prompted researchers to conduct several research projects surveying and investigating the security issues associated with Vehicular ad hoc network (VANET), ITS, interconnected vehicles, and autonomous vehicles, as shown in Table 1. These research projects also identified possible threats and attacks on those systems, along with their detection mechanisms. For example, Sakiz *et al.* [19] compiled the potential attacks on VANETs and their detection mechanisms, while the safety failures and security attacks on an autonomous vehicle and the corresponding mitigation strategies were discussed in [20]. Some of the attacks were identified in the studies presented in [20] as probable attacks, but they occurred later in recent years. The investigation of the actions to data interference attacks created via a model is also presented in this research. Moreover, some research was performed well by two people regarding ways of hacking ethically to a Jeep Grand Cherokee [21].

The attacks on self-driving cars can allow attackers to control, manipulate, or suppress the information being routed in the network. This control over the information of the users can be used for their benefit or completely disrupt the network [3]. For this reason, a survey conducted in [21] shows that, even though the majority of people of the UK, the USA and Australia had a positive general impression about a self-driving car, their major concerns are riding in it, its security issues and fully autonomous driving. Therefore, these concerns create a strong appeal to the relevant researchers to compile and analyze attacks that already targeted self-driving cars so far. From the lessons learned and the predictive analysis of potential future security threats for self-driving cars and ITSs, it is important to establish reliable and effective protection mechanisms against the security threats before putting the self-driving cars on roads [22], [23]. Even though self-driving cars will be integrated with complex and effective security mechanisms before hitting the road, they can still be under cyber-attack while operating as the attackers will also explore more complex attacking tools. Considering that, a new wave of research works is emerging, emphasizing on the resilient operation of self-driving cars under cyber-attacks [24]–[32].

However, as shown in Table 1, up to now, there is no survey paper on the real-life attacks on self-driving cars in an ITS. In this paper, the studies that have pinpointed the vulnerabilities and the potential approaches to mitigate them are reviewed and analyzed. Besides, considerable efforts have been made by the research community to assess the impacts that may manifest when a vehicle or related infrastructure becomes compromised. This survey paper discusses the threats and weaknesses related to various sensors, controls, and data communication technologies that are currently in the market and the proposed/planned technologies that are highly likely to be marketed. This paper also reviews the major reported attacks that targeted self-driving cars and ITS. This survey highlights that most of the research work on the security issues relating to self-driving cars are reactive, and thus friendly adversaries, often identify major vulnerabilities. The research gaps in securing the state-of-the-art self-driving car technologies have been identified. These research gaps emphasize the importance of addressing many issues to protect self-driving cars and CAVs from future cybersecurity threats. Nevertheless, a summary of the main contributions is given below:

- We cover the cyber-attacks that originally happened on self-driving cars and classify them based on the cybersecurity taxonomy. The vulnerability of the system or components of a self-driving car exploited by hackers and the name, impact, and type of attacks and their violated security issues are detailed in this survey.
- This paper also presents the mitigation approaches adopted by the manufacturers after having those cyber-attacks. Furthermore, we have recommended suitable mitigation approaches when they are not articulated by the manufacturers. Besides, the government policies or laws introduced by the countries across the world to legally preventing attacks on self-driving are also described.
- This survey includes recent works on how a vehicle can ensure resilient operation even under ongoing cyber-attack leading to on-road safely when vehicles are operated driver-less in future. Such works have not been systematically discussed and analyzed in previous surveys.
- Finally, we outline research directions to further hardening of security to combat recently reported and potential future cyber-attacks.

The rest of this paper is organized as follows: Section II discusses the current ITS applications, architecture, and entities. In Section III, we have presented the ITS standards and projects. The ITS security requirements and architecture is presented in Section IV. Recent attacks on self-driving cars in ITS and their countermeasures are discussed in Section V. Some of the other possible attacks on an ITS and the countermeasures of these attacks are introduced in Section VI. Section VII presents the resilient operation of self-driving cars under cyber-attacks. This paper concludes with a discussion about the research gap, and future research is given in Section VIII.

## II. ITS APPLICATIONS, ARCHITECTURE, AND ENTITIES

Self-driving cars not only take autonomous driving decisions by utilising their sensors' inputs, but also can communicate with other vehicles on the road and with the whole traffic system. ITS encompasses the whole echo-system of on-road traffic which can ensure better road operation and safety. Over the last two decades, researchers are stressing on the importance of VANET - the vehicle to vehicle communication. With introduction of self-driving cars, VANET will be an integrated part of ITS system, where the autonomous vehicles

**TABLE 1. Summary and scope of survey works on autonomous vehicle security.**

| Topic | Year | Scope | Real-life attacks | Possible attacks | Simulated attacks | Security issues |
|---|---|---|---|---|---|---|
| Public view on self-driving vehicles [22] | 2014 | Reviews people's thoughts concerning self-driving vehicle technology in countries - (i) USA, (ii) UK, and (iii) Australia. | ✗ | ✗ | ✗ | ✗ |
| Review of attacks on intelligent transportation systems and the detection mechanisms of those attacks [20] | 2016 | Discusses the classification of attacks based on their effect and the relevant detection technique. | ✗ | ✓ | ✓ | ✓ |
| Progression of autonomous cars and vehicular fogs from the intelligent grid [34] | 2015 | Details the resources and virtual platform of a vehicular fog and its associated security and privacy issues from the perspective of an autonomous vehicle. | ✗ | ✓ | ✗ | ✗ |
| Possible attacks, exploits and vulnerabilities to autonomous vehicles [35] | 2018 | Outlines the possible vulnerabilities of connected and autonomous vehicles and their recommended protective mechanisms. | ✗ | ✓ | ✓ | ✓ |
| Different aspects of a cyber-physical system [36] | 2017 | Discusses various aspects of smart components and systems, and security issues of a cyber-physical system. | ✗ | ✓ | ✓ | ✓ |
| Impact of cyber-attack on the wireless communication technologies used in an ITS [37] | 2019 | Presents recent and significant cybersecurity issues affecting many areas of wireless communication networks used in VANET and ITS. The cybersecurity resilience of a futuristic VANET/ITS model is also estimated in this paper. | ✗ | ✓ | ✓ | ✗ |
| Review of cybersecurity of CAVs [38] | 2018 | Details various security challenges that may be encountered by CAV. These challenges include diverse types of passive and active cybersecurity attacks. This paper also presents potential protections against these attacks. | ✗ | ✓ | ✗ | ✓ |
| Safety failures and security attacks on autonomous vehicles [21] | 2019 | Highlights the studies that focus on the safety failures and security attacks of an autonomous vehicle and their possible solutions. | ✗ | ✓ | ✓ | ✓ |
| Review and classification of automotive security attacks [39] | 2019 | Categorizes the security attacks on autonomous vehicles using a new classification taxonomy that can represent attacks in a better way for the concept development and testing an automotive system. | ✗ | ✓ | ✗ | ✓ |
| Chowdhury et al. (This survey) | 2020 | Discusses the recent attacks that have been reported/demonstrated on self-driving cars, the adopted or possible mitigation approaches, and most importantly highlights techniques proposed to ensure safe and resilient operation of AVs even when a vehicle is currently under attack. This paper also outlines government projects and initiatives for preventing vehicular networks from cyber-attacks compared to existing surveys. The paper further elaborates future research directions to combat security vulnerabilities. | ✓ | ✓ | ✓ | ✓ |

will communicate with each other to take collaborative decisions on road. Through VANET, any observation by an ITS unit (a car, RSU or IoT sensors) can be propagated to other vehicles, which leads to creation of interesting applications of ITS systems such as traffic management and road safety. Wireless protocol 802.11P has specifically been designed for vehicle to vehicle communication to allow the AVs to form a network. However, security issues arise when such communication happen on an open channel, thus security measures need to be taken to make VANET communication secure to ensure a successful ITS system operation. In this section, we will shed some light on the possible applications, architecture and entities of an ITS system and VANET [39].

### *A. ITS APPLICATIONS*

ITS systems use vehicle data collected to enhance car use, traffic safety and passenger comfort and standardise the use of infrastructure projects. ITS implementations can be mainly classified into four key groups as shown in Figure 1, ITS applications can be broadly categorized into the following four main classes [40]–[42]:

- infotainment and comfort
- traffic management
- road safety
- autonomous driving applications

Overview of these application classes are described in the remaining section below.

#### 1) INFOTAINMENT AND COMFORT APPLICATIONS

The objective of these applications is to enhance a valuable driving experience to drivers through services that meet their needs. There are Trusted Service Providers (TSPs) of services whereby the applications are accessed after downloading and installing them on a car's data center using Onboard Unit (OBU). A classic example is that of the applications which offer universal Internet car's commuters access to ensure that clients travel feeling comfortable and relaxed as they can access online streaming of videos or gaming, among others. Such applications rely on communication channels with a latency of below 500 milliseconds' [43].

#### 2) TRAFFIC MANAGEMENT APPLICATIONS

Commuter traffic control applications exemplify a leading grouping of applications of ITS. Vital intentions of this form of application are to:

- strengthen traffic flow control and synchronization, and
- provide drivers with cooperative traffic services.

Such applications rely on collecting and analyzing the messages exchanged by ITS entities (refer to Section II.B.2 about the details of ITS entities) to create and manage overall traffic map databases. Traffic data is usually obtained by the RSUs deployed and the road sensors. The data obtained for further processing and interpretation was wirelessly transmitted to trusted distributed data centers. The data provide detailed information concerning cars, drivers, and incidents on the roads.

As soon as the data is processed and interpreted into important data, it is conveyed to motorists via service suppliers to alert them of the existing congested zones, commended routes, steering directives. Additionally, these streams of traffic control applications aid the established order to implement an innovative stream of traffic facts scrutiny similar to an Origin-Destination (OD). The OD journey matrix targets at approximating traffic flow capacities amid diverse backgrounds and endpoints [1]. Road traffic administration applications depend on intermittent wide-ranging performers of security mails among other Vehicle to Everything (V2X) communications that have a latency of fewer than 200 milliseconds. Samples of additional applications comprise governing swiftness limit warning, emerald light optimum swiftness advisory, automated toll assortment, as well as car public road administration [2].

These ITS applications enhance the stream of transport flow in urban areas public highways, which are widely encompassed into lane control, highway surveillance, parking lots management, and roundabout intersections points. Reconnaissance applications are more distributed to dualistic classifications [20]. The first category is fixed reconnaissance systems, which comprise of fixed locations which use cameras as well as sensors which are connected on the highways to screen highway settings. The other category is known as reconnaissance on the highway. It uses radars and visual cameras entrenched in cars to sustain surveillance. Road control applications concentrate on an organization the existing volume of the highways all through different traffic situations like emergency departures, sudden events, or hazardous meteorological conditions RADAR is used as well as cameras, and ultraviolet sensors which sense dwelling, route, and speed of automobiles [44]. Distinctive event carriage controlling structures are a disparity of road control structures: these systems control and decrease highway jamming complications at distinct dwellings like arenas or bond hubs. The sensors like radar, which are infrared, as well as cameras, enhance the flow of direction and enhance the shift of routes on transport demands. Intersection points administration applications are supportive applications which are a feasible spare of the outmoded traffic flow lights built intersection control. Here, the highway users, as well as traffic management and infrastructure centers, work together as a combination of radars, cameras, sensors, advanced Radio Frequency Identification (RFID), high-tech, ultrasonic, and simulated traffic beams to enhance transportation [45], [46]. Parking Management Applications (PMAs) are enhanced through the use of RFID high techs, among other inductive coils technology, and it's the technique used to collect data on car parks, unfilled spaces in the parking lots, and yellow curbs zones. With such advanced applications being on the rise, there will be better space utilization in parking spaces. This will meet all drivers' needs and reduce commuters' frustration of car jams and other issues caused in the parking zones.

Those applications need to articulate an essential as well as a shared structure to allow the ITS placement. In this fast-evolving world, we require improved road traffic control with a comprehensive outlook on the public and also the shareholders. For example, assuming that a town has a huge occasion, therefore; a road traffic professional chooses to create certain guidelines to reduce congestion. Road control application transforms the total traffic lanes in similar routes, varying to improve entrance on the way to the occasion. However, the vital problem (reduced congestion) is not resolved since many individuals will need parking spaces, and this will increase congestion since the intervals required to get a car park spot becomes impossible. Lack of a parking spot is among the causes of regular all applications incorporation. Here, the line of traffic controls and car park controls applications might interrelate to disperse an automatic car park spot and save on time. Road security application setups have been integrated using the information technology systems. This minimizes accidents and cars getting congested and stuck in traffic, especially during hours of leaving work towns to get congested. As a result, all mechanisms of information technology systems sporadically direct security e-mails to prepare the environs about vital traffic data of the zones as well as speed data. Additionally, on the topic of assured happenings similar to accidents, the ITS signals the automobiles as well as emergency facilities within that locality through a communication network. Significantly, the end-to-end message investigates one of the important units for highway security


**FIGURE 1.** ITS Applications.

applications. As presented in Figure 1, there are four diverse samples of the ITS highway security applications;

- Emergency car
- Accident warning
- Diagnostics
- Signal abuse warning

An illustration of an accident warns there is a person crossing the road; thus, the application warns the driver of pedestrians crossing; thus, the car stops. The sensors act as the main control center in this application. For instance, the sense that pedestrians are crossing by detecting even those walking on sidewalks; thus, this prevents cases of accidents occurring. RSU sensors have the ability to detect every movement on highways, be it the sidewalks or on the main road, and it acts as an accident forecaster. This is the main application for such sensory activities, but there are other applications that serve the same detection purpose as an application called left-turn drivers' assistance system. Just like the name of the application suggests, it aids all assistance to drivers injunctions or roads that intersect, thus aids in taking left turns in such junctions. For accuracy in detecting the chances of these occasions, the RSU application gets data from OBU, and other road detectors and sensors in the car, thus prevent collisions. There is an application for cars called Intersection Violation Warning System (IVWS), which was established in the year 2008 from the United States of America Department of Transport (USDOT). This act occurs especially injunctions and places with ease of ignoring traffic signs and traffic lights; the prototype IVWS comes in handy in such events. The same prototypes also detect when drivers are at risk of ignoring traffic lights, and it's all empowered by sensors as well as other sensors and improved setups. The navigation of cars and how Global Positioning System (GPS) work at intersections also relies on some algorithms built on several prototypes and information technology systems. They help in the determination of risks that are caused by collisions or unexpected intersection road fatalities. With such high-tech advancements, there will be a fast response to emergencies since emergency cars that have sirens requesting the right of ways, such as ambulances or police cars, can easily communicate with self-driven cars and request right of way. Motorcades will no longer be an issue that causes congestions with this advanced technology on the highways. The ability of cars to communicate will lead to reduced collision cases breaching road rules and other collisions that are mostly caused by irresponsible driving.

### 3) ROAD SAFETY APPLICATIONS

The vital rule of roads is to ensure both the passengers and the drivers are safe; thus, some applications are used through information technology systems that have enhanced road safety aspects. V2X wireless communication is the main application used to enhance road safety. Consequently, it's an interconnection of all information technology systems that enable conveyance of signals and messages to control car speeds depending on the surrounding locations and highways

activities. The applications also send signals when in cases of accidents, alerts, and all sorts of emergencies and the communication used is called a multi-hop. For encrypted information from end to end to be enabled, it needs an advanced flow of communication through high tech advancements. The significance of these applications is that highway safety, as well as safety of the pedestrians and drivers, is enhanced [9]. Archetypes also sense when drivers are at a possibility of paying no attention to traffic lights, and it's all sanctioned by antennas as well as other sensors and upgraded setups. The celestial navigation of carriages and how GPS structures work at crossings also depend on a certain set of rules put up on several prototypes and information technology systems. They aid in the determination of threats that are triggered through crashes or unpredicted intersection highways death tolls. With such high-tech developments, there will be a dissolute response to tragedies since the emergency carriages that have danger signals demanding the right of ways, such as ambulances or police cars, can with no trouble communicate with self-driven cars and demand right of way. Convoys will no longer be a problem that affects car overcrowding with this innovative technology in the freeways [40], [41].

#### 4) AUTONOMOUS DRIVING APPLICATIONS

With this significant advancement of the most anticipated self-driving cars launch, many applications are being set up in this decade, and these applications are called self-driving applications. Figure 2 shows the innovative technologies used in self-driving cars that ensure drivers are not compulsory for complete mechanization of a car as in these cars, the driver becomes the traveler like other passengers. These cars rely on automobile recognition as well as other driving roles embedded in six robotics stages. Different tools are integrated into the program driving cars encompassing Lidar, as well as radar, which prevents mishaps by generating a 360 gradation field outlook. The ultrasonic sensors sense incidences of obstructions, which include crossing people or animals, among others. These cars use considerably the vehicles acquired by the Global Navigation Satellite System (GNSS). It is still the GNSS system that promotes communication with proximate cars, distant service providers, highway setups, and essential events through communication tools called V2X [22], [23], [47].

Furthermore, cars with self-driving know-how offer a variety of benefits, for instance, protection against vehicle robbery, mishaps, and accident reduction. They also lead to a decrease in transportation overcrowding, as well as the escalation in public road car parks. Through the advancements in the information technology systems enhance a safer and secure communication between the developed interfaces. Unquestionably, security applications need the sporadic distribution of secure connections to discover the risky road points, detect, and inhibit the danger of accidents among vehicles. Also, cyber-attacks may influence self-driven automobiles' performance leading to mishaps, mainly when there is an interruption in the communication streams of the autonomous vehicles. Succeeding chapters are discussing more on the information technology systems projects, ITS standards, the architecture, and all featured risk analysis, potential threats, and prevention measures [40].

### B. ITS ARCHITECTURE AND ENTITIES

#### 1) ITS ARCHITECTURE INVOLVING SELF-DRIVING CARS

Figure 3 shows the ITS high-level structure consisting of three primary domains: (i) vehicle, (ii) V2V, and (iii) infrastructure domains, and their inter-communication such as in-vehicle and V2X (e.g., V2V, V2I/I2V) communication.

There is an OBU, which is mounted inside vehicles on an IN vehicle domain to enhance the flow of communication between these applications. V2X realm generates an ad-libbed system within OBUs and the RSUs, which are organized along with the highways, ITS path, and railing networks. Communications amongst OBUs and neighboring pedestrians are different vehicular message tools (V2X), which are wireless means of communication used as soon as the data collected by OBUs has been exchanged instantaneously with adjoining ITS units. Some prototypes are displayed regarding the pedestrians' interface as well as that of RSUs. The central aspect of these automated vehicles field is RSU. They are positioned on roadsides or yellow curbs. Every car connects the adjoining RSUs via the cars' OBUs. Consequently, RSU is acknowledged as a connection amongst vehicles. A setup field of these cars also integrates the Trusted Third Parties (TTP) like car producers, as well as TAs trust establishments. TAs doesn't entirely trust; hence minor long-lasting RSUs can be deliberated as connections joining additional conveyance tools and vehicles. Specific applications use the incorporation of system technologies that form an interrelated means of transportation. For instance, junction accident warning, incorrect driving warning, as well as secluded vehicles are all detected through applications. These applications are generally acknowledged as intellectual transport structure applications. Vital portions of the apps include the AU, the OBU, as well as the RSU [41], [41].

RSU correspondingly performs roles of host applications that offer services, but an OBU is a viscount device that uses the facilities delivered by RSU via Application Unit (AU); hence this application may be situated in an OBU or RSU. Moreover, every vehicle is fitted out with sensors that collect data successively and conveys it as communication to other vehicles in wireless forms. The RSUs are dispersed consistently while the program array of cars is greater than the entire scope of highways. Thus, the situation of a vehicle isn't affected by communication. RSU or OBU Contains three base keys [43];

- Private Key
- Public key
- Shared key

The way the keys are distributed in RSUs, and OBUs, is to prevent any form of the cores from being tampered with by users. Some cars do need the applications for data

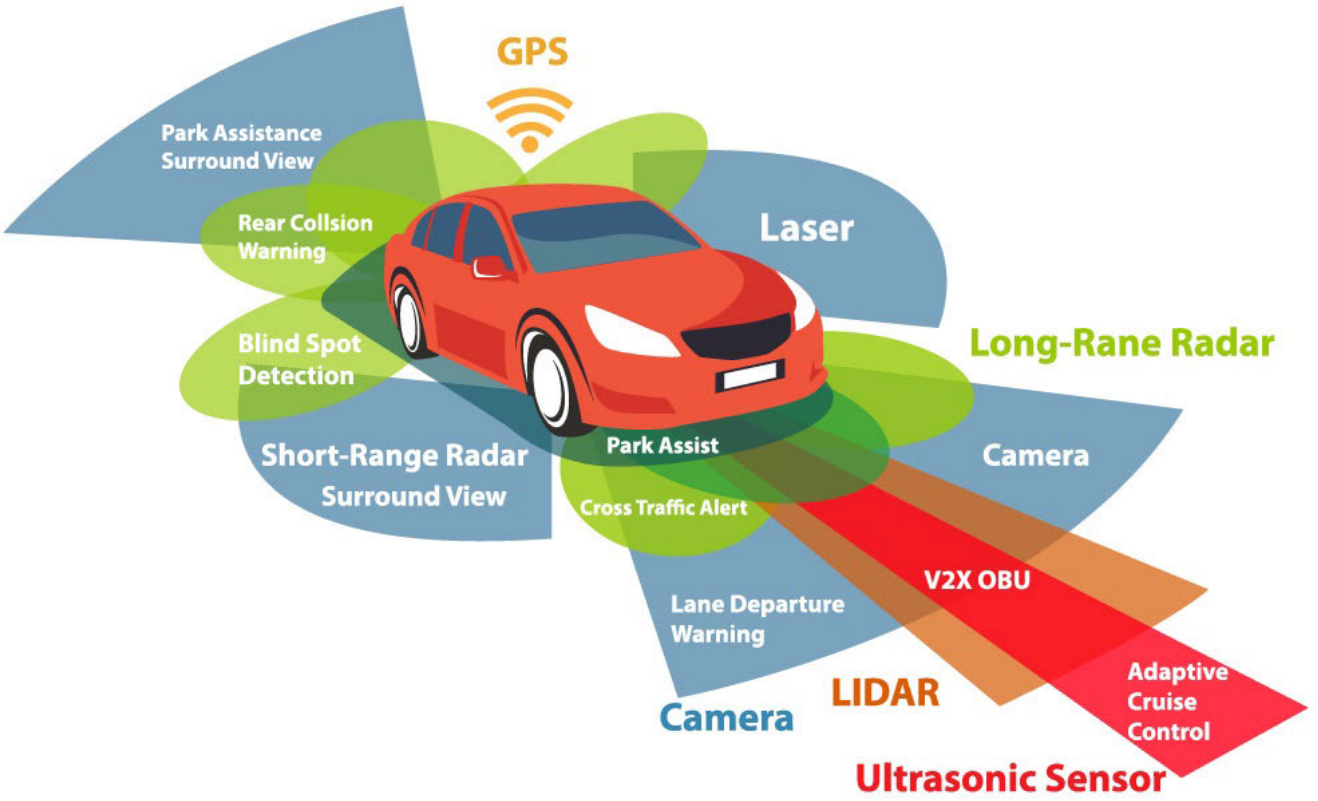


**FIGURE 2.** Key enabling technologies of a self-driving car.

verification and many encryption performances of communication amongst cars for a clear understanding. Communication is enhanced through RSUs as well as the OBUs, which are linked in all vehicles to ensure effectiveness, especially when emergency cars need the right of way. Through these links, all vehicles can communicate hastily, and it's efficient in urgent scenarios of transport. The advancements that have been occurring in the technological world are playing vital roles in the development of self-driven cars. It has been the best thing that has happened in the history of transport globally [48], [49].

### 2) ITS ENTITIES

From a security perspective, a number of different actors may be interested in an ITS network [50]–[52] that includes drivers, OBUs, RSUs, third parties, attackers, and infotainment systems. The description of these entities are given below:

**Drivers**: Drivers are the chief fundamental entities in ITS structures as they create vibrant resolutions and interrelate using the systems that drive support to make sure that there is a fast and safe drive. Self-driving vehicles need a driver as much as it's called automatic for safety reasons in several countries.

**Onboard Unit (OBU)**: Critical functions of Onboard Units are wireless hi-fi access, information security, dependable communication transfer, topographical direction-finding, and Ad hoc system jamming control [53]. As Onboard Units offers equally Vehicle-to-Infrastructure (V2I) as well as Vehicle-to-Vehicle (V2V) communications, it must be fitted out with many wireless hi-fi access tools to guarantee consistent messages amongst V2V as well as V2I. Onboard Units may frequently convey status communications to additional Onboard Units to sustain security applications necessary for vehicles. Later the first information remains overwritten. Onboard Units is fitted out with a room that records events administered, reported, and communicated to other OBUs like a black box in an airplane, which keeps track of all the message information for a specific flight. Diverse varieties of vehicles use various storage services, similar to the adaptive road traffic incarceration structure. It stores the stream of traffic data, e.g., the total vehicles overlapped at junctions, as well as pedestrian information to offer enhanced and operational road traffic administration services [54], [55].

Onboard Units also comprise peoples crossing points, a specific interface that links to other Onboard Units, as well as a systematic method for small varieties of wireless messaging built on the IEEE standard. Onboard Units

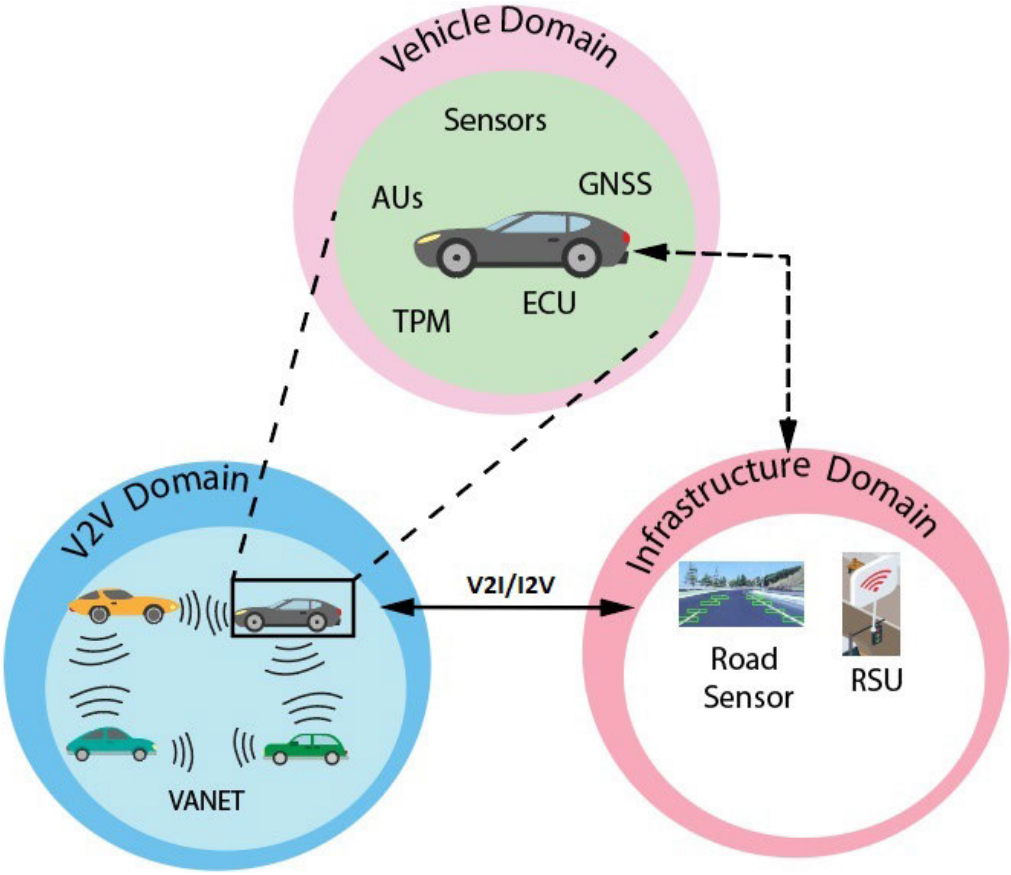


**FIGURE 3.** ITS architecture for self-drivng cars showing main communication domains.

also encompasses 5.9 GHz devoted Tiny Range Message transceiver called the DSRC, Electronic Control Unit (ECU), an AU, application CPU, Human Machine Interface (HMI), and GPS structure (refer to Figure 2). Several ECUs on nearby vehicles join forces by substituting communications with particular Onboard Units as well as AU to form an onboard system. Application Unit (AU) is a device fitted out in a car that uses applications that offers remote services through the communication units of a connected OBU. Communication means amongst an OBU and AU it is wireless or underwired. AU converses via the system solely through its Onboard Units, which is responsible for movement and interacting functions. For that reason, Onboard Units manages transfers using the system connector. AU converses with additional adjoining ITS units using its connected OBU. It may exist as a devoted safety device application or a distinctive device like a particular ordinal associate to route through the Internet [56].

Vehicle TPM aids safe and resourceful communication as well as managing several sources and documentations. HMIs are collaborative and non-intrusive. They have to be avoided by a motorist during driving. Consequently, Onboard Units should need a touch VDT that controls how it uses it when a vehicle is in motion. Also, to facilitate its use all through driving, a vocal sound built communication has previously been encompassed in vehicles to escape the commotion. Lastly, the GNSS entity takes the locality of a car [57].

**Road Side Units**: The routing protocols used in a VANET are proactive, reactive, and hybrid in nature.

The main functions of an RSU are to:

- extend the communication range;
- provide Internet connectivity to OBUs; and
- equip with safety applications such as accident warnings.

As mentioned before, in ITS, OBU and RSU communicate with each other. As shown in Figure 3, the communication between RSU and OBU is bidirectional and can be wired or wireless. Table 2 lists various technologies used in the ITS.

- Third-party entities: This type of entity can be trusted given full conviction and are set to accomplish the digital certificates, public key pairs, and the several hidden ones. An excellent example of these includes conveyance monitoring agencies and vehicle manufacturers.

**TABLE 2. Enabling Technologies in ITS [58], [59].**

| No. | Technologies | Systems |
|---|---|---|
| 1 | Communications | Wireless wide area networks (Cellular, MANET, LPWAN) and wired line (coaxial or fiber Optic) |
| 2 | Data storage and processing | Compact and hard discs, magnetic storage and media magnetic stripe cards, hard disc disks, data cartridges, smart cards. |
| 3 | Database management system | Data warehousing and expert systems |
| 4 | Information Display | Cathode-Ray Tubes (CRTs), LCDs and variable message sign |
| 5 | Location | Dead reckoning, map matching, GPS, beacon based vehicle location |
| 6 | Sensors | Inductive loops, infrared beams, microwave (Radar), Lidar, computer vision sensors and acoustic scanning laser |
| 7 | Actuator | Automated steering, headrest, viewing glasses, door adjustment |

- Attackers: Attackers attempt interfering with the security of the ITS through the use of more advanced expertise attacks.
- Infotainment system: A vehicle is equipped with various entertainment units such as FM radio, games, and a sensor network. The sensor network is used to monitor the driver's physical parameters (e.g., heart rate, temperature). The data from this network are collected by an OBU for later analysis. Users' gadgets such as PDA or cellular phones can be used as an interface to generate information or to receive data from the vehicle or external devices. A user can export data to his own laptop at home and store all the information generated in a journey.

## III. ITS STANDARDS AND PROJECTS

Work and standardization efforts on ITS started substantially about a decade ago. These standards have been in existence for over one decade, and they define the architecture references through ITS. This study and all the undertakings encompass many multidisciplinary capacities, including wireless channel demonstration, information link conventions, wireless infrastructures, networking conventions, safety, information privacy, as well as localization. In this part of the research, there is a brief demonstration of the best and significant ITS calibration activities, hi-tech skills, as well as research schemes.

### A. ITS KEY ENABLING STANDARDS

The dissertation of the aggregate demand was aimed at improving the applications of ITS. IEEE802.11p duty group was molded in the year 2004 in the direction of providing modifications and improvements to the IEEE802.11 private standard, which supports the Wireless Access in Vehicular Environments (WAVE). This standard was made available in the year 2010. It permits usage of authorized ITS orchestra of approximately 5.9GHz frequency to facilitate V2V messaging between extremely mobile vehicles as well as V2I messaging between RSUs means of transportation. It's eminent that IEEE802.11p explains just the provisions for basic physical (PHY) as well as the Medium Access Control (MAC) covers. [60].

IEEE802.11p cover is established on an Orthogonal Frequency Division Multiplexing (OFDM) technique using 10 MHz frequency bandwidth backup for several information rates. IEEE802.11p stratum is built on Enhanced Distributed Coordination Function (EDCF), which are improved distributed synchronization functions used with the current IEEE802.11 criteria. EDCFs maintains the features of all quality provisions, safeguarding extraordinary precedence for inactivity-sensitive mails, e.g., the ITS security messages. IEEE operational group was designed to outline additional advanced layers that have various uses. This group created in 1609 (1609.1, 1609.2, 1609.3, and 1609.4) is created to examine and analyze more ranked layers above [61], [62]. The combination of the standards IEEE 802.11p and IEEE 1609 is widely known as WAVE.

Specific current standardization efforts are also being undertaken in Europe through the ITS technical committee working group of the European Telecommunications Standards Institute ( ETSI). The ETSI ITS specification describes a co-operative vehicle communications reference architecture covering six key layers [63], [64] :

- The application layer for handling ITS applications in general, including ordering and sorting,
- The facilities layer support sessions as well as information presentation,
- The web and transportation layer consists of Geo–Networking, transport protocol,
- The standard access stratum supports several communication mechanisms,
- The administration unit manages the structures of the ITS design layers, and
- The safety entity offers security amenities, e.g., validity, data discretion.

### B. ITS RESEARCH PROJECTS

ITS is an interdisciplinary and cross-sectoral research field that can only be accomplished by large-scale research projects with a team of researchers from different disciplines. For this purpose, research on ITS typically includes large-scale research projects. This section summarizes the most critical research projects already completed or currently involved.

#### 1) COMPLETED ITS PROJECTS

Projects that have been completed so far are:

- Open vehicular secure platform (OVERSEE - EU/FP7): The undeveloped vehicular protected policy Apprehended an exposed and ordinary amenable in-vehicle platform that facilitates the improvement of safe

applications of ITS and authorizes ensuring total segregation between self-governing applications.
- e-safety vehicle intrusion protected applications (EVITA EU/FP7): e-Safety for ensuring the safety of vehicle communication architecture, which is vigorous to cause frustrations to ant attacks and offer full protection to confidential data within the car.
- Privacy aided ability in supportive systems, as well as security applications, analyzed discretion related matters in supportive vehicles and highway safety structures, were studied, and gauge.
- Intellidrive for safety, mobility, and user fee project (Intellidrive - U.S.): Intel drive for protection, mobility, and consumer fee scheme was designed to study innovative security tools for V2I and V2V infrastructures as well as their deployment experimenting.
- SafeSpot project (EU/FP6): Safe Spot schemes were considered on various interacting, and other tools for V2I dispatch were premeditated.
- Secure vehicle communication project (SEVECOM - EU/FP6): Safe vehicle report scheme introduced safety design, procedures, and tools for ITS communication structures, comprising identity administration, information consistency, and confidentiality as well as performance valuation.
- Co-operative vehicles and highways for nontoxic and smart transportation schemes were developed to advance dispatch procedures and interacting amenities to improve the information transmission over V2I connections, and they were evaluated using a standard amenable platform.

In recent years, several new research ventures have been initiated or are still underway. There are some outstanding examples in the following section.

#### 2) ONGOING ITS PROJECTS

- COMeSafety2 project (EU/FP7): this project aim is to enable the growth and deployment of supportive ITS security applications as well as promote some of their returns towards industrialized authorities.
- Formulating safe V2X dispatch schemes project goal is to plan, improve, and appraise safe and accessible V2V communication structures in disposition scenarios.
- Innovative cellular tools for linked automobiles project purposes to improve new policies to link IEEE802.11p using LTE in the direction of improving the system performance as well as enable interruption forbearing services.
- Co-operative schemes for hi-tech mobility facilities and resolutions project purpose is enhancing highway traffic proficiency by offering new supportive and factual traffic information assortment and distribution concepts.
- Security and safety modeling project (SESAMO - EU/FP7): The safety and security modeling scheme's objective was to examine, apprehend, and perfect the associations between practical security and safety devices in entrenched systems.
- Scalability and reliability engineering-based vehicle technologies for secure and smarter roads (SafeITS - Qatar National Research Fund): Engineering safety and presentation aware autonomous vehicle applications for smarter highways strategies are to plan adaptive and framework applications of ITS. It will enable the dynamic variation of service quality and safety structures to guarantee the security of ITS operators and units. [65]–[67].

The completed and current ITS projects presented in this section show that one of the main objectives of almost all projects is to ensure security and privacy. Security and privacy issues are observed as an obstacle to the widespread acceptance of ITS systems and self-driving cars. Research on all these issues has, in the last decade, gained much interest from the related research community. The ITS Safety specifications and architecture are described in the section below.

## IV. ITS SECURITY REQUIREMENTS AND ARCHITECTURE

The ETSI ITS standard is currently operational in the European countries. In this standard, security has been added as one of its communication layers. In the first place, ITS technology was developed to improve road health, passenger safety, and traffic quality. Since it relies heavily on wireless communications, however, many threats may disrupt its operation and thus cause serious accidents. A list of possible security threats on different ITS components, along with their direct impact and consequences on creating traffic hazards, are presented in Table 3. For example, for 'infrastructure sign' ITS component, possible threats could be change/add/remove road signs (e.g., speed limit, irrelevant message). The direct impact of these threats is either the false reaction or no reaction (False/No reaction) of a vehicle, while these threats may create hazardous situations like disturbance, collision, and congestions.

To protect from these security threats, several security requirements have been identified, which are described in the following section.

### A. ITS SECURITY REQUIREMENTS

The effective distribution of ITS structures in practical applications needs diverse safety requirements to make sure secure communications produce safe experiences of driving. Hence, the scheme of security requirements of its applications requires distinctive consideration, and it's described by detailed tests and safety requirements. [68]–[71]. The detailed discussion of these requirements is given below:

- Authentication: This is the key ITS safety provisions, which is categorized into these requirements: (i) User verification to inhibit Sybil occurrences and terminate malicious units (ii) Source verification to make sure messages were produced by genuine ITS units (iii).

**TABLE 3.** Possible threats on ITS components and their impact and consequences of creating hazardous situations.

| ITS components | Possible threats | Direct impact | Hazardous situations created |
|---|---|---|---|
| Infrastructure sign | Change/ add/ remove road signs (e.g., speed limit, messages) | False/ No reaction, | Traffic disturbance, collision, and congestions |
| Radar/Camera | Creating blind spot and presenting false image | False reaction | Driver disturbance |
| GPS | Spoofing and jamming | Inaccurate location information and wrong maneuver | Traffic disturbance and crash hazard |
| In-vehicle devices | Malware and head unit attack | Depends on malware capability | Serious traffic congestions and driver/traffic disturbance |
| Acoustic sensors | Interference and fake sound | False positive/negative obstacle detection and sensor malfunction | Traffic disturbance and low/high speed crash |
| Lidar | Jamming and smart material (absorbent, reflective) | False detection and degraded Lidar performance | Loss of situation awareness and traffic disturbance |
| In-vehicle sensors | Eavesdropping and malware | Privacy leak, reverse engineering and false message generation | Traffic disturbance, disabling vehicle automation service and accident |
| Infrastructure (RSU) | Denial of Service and fake WSA (RSA, SPAT) | Wrong notification to driver, wrong detection and no information for ITS | Traffic disturbance, safety issues and critical incident |

Location verification protects the reliability and significance of current data.

- Data integrity: All units of ITS ought to be capable of verifying and authenticating the reliability of conventional communications to inhibit any unlawful or mischievous operation and obliteration during communication.
- Data confidentiality: Swapped messages must be well encoded and secured to inhibit the leak of delicate data to mischievous nodes or unauthorized parties.
- Privacy and anonymity: The uniqueness of car owners and cars shouldn't be straightforwardly seen from the automated communications channels. It's the right of the car drivers to use personal information and share it with whoever they want.
- Availability: Exchanged data ought to be managed and prepared instantaneously, thus necessitating the execution of minimal overhead as well as insubstantial cryptographic processes.
- Traceability and revocation: ITS establishments ought to be capable of tracking mischievous ITS units that abuse ITS structures and rescind them quickly. When a difference of opinion arises or a mischievous autonomous vehicle is spotted, TA discloses and retracts its distinctiveness, and it's added to the cancellation list.
- Authorization: It's essential to outline access regulation established on permission privileges for diverse ITS units. Specific procedures must be applied for logging in or negating access to specific ITS groups, individual tasks, and information use.
- Non-repudiation: All ITS units must be exclusively connected to their data and activities to accomplish data validity and initiation.
- Robustness against external attacks:: ITS units must be full-bodied against several peripheral attacks, and the software of ITS must be free of susceptibilities and prudence flaws.

For the fulfillment of the above-mentioned security requirements, several global security architectures for an ITS system [72]–[74] have been developed. The following section describes those architectures.

### B. ITS SECURITY ARCHITECTURES

The current ITS security system architectures can be classified into three main different cryptography-based categories: (i) Public Key Infrastructure (PKI)-based architectures; (ii) crypto-based architectures; and (iii) ID-based architectures.

1) PKI built safety designs depend on distorted encryption systems to offer several safety services like credential generation, validation, distributing, revitalization, examination, appraising, and annulment. An official document delivered by a PKI associates the unrestricted key using the proprietor's identity data in addition to encryption tools. PKI preserves a document cancellation list to guarantee protected administration in actual network settings. This prerequisite may be considered as a dismal feature of ITS systems and leads to extraordinary communication levels. A comprehensive list of contemporary PKI established security systems and their valuation is presented [72].
2) Crypto based safety architectures is usually centered on both symmetric and irregular encryption systems to offer several safety services. An illustration can be how these designs offer an innovative ITS safety system that provides confidentiality, information privacy, and reliability, and non-repudiation using an irregular block cryptogram system and a document-based unrestricted key encryption system. The solitude and information discretion are guaranteed using full-bodied block encryption that is the Advanced Encryption Standard (AES).
3) ID-based safety designs reduce other approaches overhead. It is done by maintaining confidentiality; an encryption system is used to create pseudonyms. This method serves the purposes of ensuring that there is

enhanced I.D. confidentiality, a requirement for user security, and confidentiality security. ID-based encryption may be used to create unrestricted solutions to units' identifiers hence moderates its results.

As alluded before, because of the high-security threat expected for autonomous vehicles, a number of attacks on self-driving cars have already been reported in the recent literature. These attacks are described in the following section.

## V. RECENT ATTACKS ON SELF-DRIVING CARS

Since the inception of autonomous vehicle drive tests, there have been various types of attacks on different units of a self-driving car, such as the internal measurement unit, Lidar, GPS, Camera, thruster monitoring unit, AU, and warning messages. There were approximately 126 incidents reported so far. In such attacks, a vehicle does not prepare a secure sequence of moves to maneuver in a tight space.

Garcia *et al.* [53] showed susceptibility to remote and accessible abuse in the case of nearly 100 million Volkswagen vehicles sold from 1995 until 2016. Volkswagen vehicles depend on several global ECU recovery keys. By intercepting one single signal from the original remote control, the attacker can thus clone a Volkswagen remote control, which enables unauthorized access to the auto. With Nissan Leaf electric vehicles, attackers demonstrated their taking control of the vehicle heater by means of vulnerabilities with the Nissan Connect mobile application, which regulates the vehicle. The battery was turned on again and again. This incident prompted Nissan to disable the application [75].

An attacker within the Wi-Fi range enabled the SmartGate application in a Skoda car to steal information [76]. Additionally, from the SmartGate system, the attacker could block the car owner. In 2015, Chris Urmson, director of the Google Self-Driving Cars project, said that if "the program sensed an anomaly somewhere in the network that could have potential security consequences, it immediately passed vehicle control on to our test driver" [77]. As mentioned in Table 4, an autonomous vehicle of the BMW 7 series could not be parked in a parking lot because a hacker had taken control of the car, causing it to run into a hit. Other attacks that happened on self-driving cars shown in Table 4 are detailed later in this section.

For self-driving cars, the operational decision is facilitated through the interpretation of the inter-vehicle communication message. Amongst the communication protocols (e.g., Bluetooth, cellular like Long Term Evolution Vehicular, 5G-VANET [78]), Dedicated Short-Range Communications (DSRC) is predominantly used in VANET. DSRC operates based on the Wi-Fi standard developed for ITSs, namely IEEE 802.11p. Recently, the security issues associated with VANET communication protocols have been emerged as prominent since if the wireless communication channels are broken, the messages can be tampered with or deleted. Such tampering or deleting message can create serious consequences, such as accidents, loss of human lives, traffic jams.

There are some recent attacks reported on VANET comprising of vehicles with autonomous Levels 1 to 4, which are not fully autonomous. These attacks include sybil attack [79], denial of service attack [80], timing attack [81], message tampering [82], illusion attack [20], and node impersonation [20]. As these attacks do not involve fully autonomous vehicles, i.e., the vehicles with Level 5 [83], therefore these are not the main focus of this survey. However, these attacks can also be possible in VANET with fully autonomous vehicles. Since the V2V messages in VANET play a key part in making driving decisions for self-driving cars, besides these, there are also some potential attacks articulated in the current literature associated with wireless communications. These attacks can be flooding attacks [84], data playback attacks [85], data alteration attacks [86], blackhole attacks [87], spam attacks [87], and cryptographic replication attacks [88]. We will present only these potential security issues of VANET comprising self-driving cars in Section VI. Figure 4 shows the different types of attacks that mainly happened in self-driving cars.

### A. MALWARE ATTACK

The first remote intrusion of a vehicle leading to cyber-physical controls against Chevy Malibu was introduced in 2011 by Checkoway *et al.* [45]. The attacker manipulated the radio of the vehicle using a Bluetooth stack weakness and inserted the malware codes by syncing their mobile phones with the radio. After the radio was hacked, a gateway system disconnected the intruder from the high-speed CAN network. However, they could repurpose this gateway from their open low-speed CAN network. Afterward, the inserted code could send messages to the ECU of the vehicle that could lock the brakes. The On-Board Diagnostics (OBD) is one of the most vulnerable parts of self-driving cars to have malware attacks. The authors in [89] showed that an attacker could use the malware-infected diagnostic tool to insert malware to ECU via OBD. These malware codes can tune and reprogram the codes of ECUs. An ECU infected by the malware may fail to respond to communicate with the other OBU components (e.g., Lidar, Camera, Radar), compromising the safety of the self-driving cars.

### B. MAN-IN-THE-MIDDLE ATTACK

Self-driving cars use wireless communication methods with other vehicles and roadside infrastructures. These self-driving cars also use wired or wireless communication methods to communicate with OBUs. In a man-in-the-middle attack, an attacker can manipulate the communication messages between the two entities (e.g., two cars of a VANET in V2V, vehicle, and RSU in V2I), while both entities believe that they are in direct communications with each other. An attacker can take control of OBU or RSU and actively eavesdrops, replays, and modifies the messages transmitted between two entities [90]. As alluded in Figure 4, the authors [91] conducted a similar assault on a Jeep Cherokee in 2015. By using the Internet-accessible weakness in Jeep Cherokee's

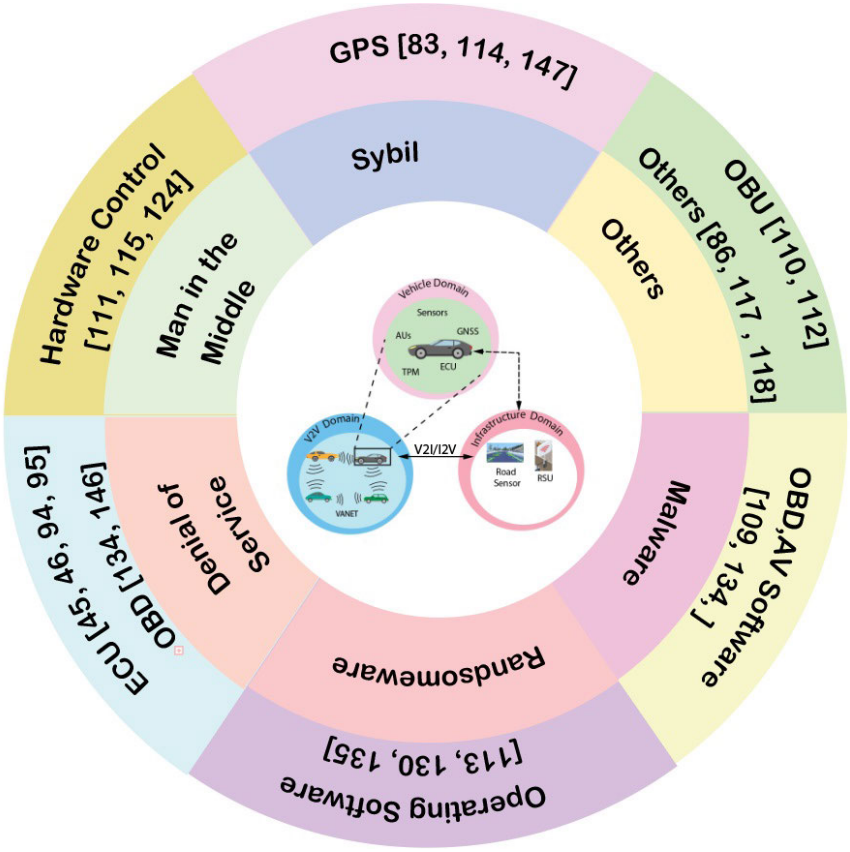


**FIGURE 4.** Classification of the attacks happened on self-driving cars. Note, attacks on VANET and ITS infrastructure have not been included here. Types of attacks are shown in the middle layer, while the outer layer shows the components of a self-driving affected by the relevant attacks.

communication method, the hackers performed a man-in-the-middle attack, and they intercepted the communication messages between ECUs and the braking system. Hackers were able to reconfigure the firmware on the central processing unit of the vehicle with CAN network access for another processor. Then they sent CAN messages that regulate the steering, brakes, and vehicle acceleration. The central processing unit was unable to detect that the instructions (to slow down or turn right) came from an external device that was manipulating the communication message between ECUs and OBUs.

### C. DENIAL OF SERVICE ATTACK

Denial of Service (DoS) attack is one of the most dangerous attacks that can happen on self-driving cars. Denial of OBU or ECU service (refer to [92] shown in Figure 4) in the middle of the self-driving car's journey can lead to fatal accidents or loss of lives. Attackers can use DoS attacks to stop Camera, Lidar, and Radar to detect objects, road, and safety signs. Braking system service can refuse service, and the vehicle may stop suddenly or unable to stop where needed. In 2016, members of Tencent's Keen Security Lab compromised the Tesla Model S remotely, taking advantage of an older version of a web browser running on the CID [93]. If they would fool a user on a malicious browser site or a car previously linked to a common Wi-Fi network (such as a dealer's Tesla Guest Wi-Fi network), they could leverage this vulnerability. Upon exploiting a weakness on the CID, the vehicle gateway system connected to the CID could be reprogrammed via Ethernet. This compromised gateway allowed them to send CAN messages that they used to hold the vehicle's brakes.

### D. RANSOMWARE ATTACKS

Ransomware attacks [ [94] shown in Fig. 4] can be a major threat to self-driving cars, mainly for commercial vehicles. The researchers in [94] showed that critical in-vehicle data such as a personal media repository, communication logs, freight monitoring logs, important control parameters, and warehouse locations could be encrypted in self-driving cars to perform ransomware attack. In 2017, Honda Motor Company suffered a major WannaCry ransomware attack. Attackers demanded a large number of cryptocurrencies to provide the decryption key. Even though this attack was not on the self-driving car itself, but it affected lots of Honda self-driving cars to get on the fly software updates during the ransomware attack. Researchers [95], [96] and law enforcement agencies like FBI warn [97] that ransomware attacks will be hackers' prime target on autonomous vehicles shortly.

### E. SPOOFING ATTACK

Attackers can perform several types of spoofing attacks like GNSS, GPS, and Lidar spoofing attacks (see [98] shown for the component ''others'' of Figure 4) on self-driving cars. Pham *et al.* [99] designed and carried out a spoofing attack against a Lidar sensor, effectively tricking the system into perceiving an obstacle in its path that was not there. The attacker sent signals shot at the victim Lidar at the nanosecond level, and the Lidar of the vehicle believed there was an object in front of the vehicle. Petit *et al.* [100] shown the efficacy of the Lidar (ibeo LUX 3) relay attacks and spoofing attacks. A cheap transceiver was able to insert counterfeit objects, which the ibeo LUX 3 can successfully detect and track. These attacks demonstrate that more techniques are needed to robust the sensor to ensure adequate sensor data quality. Eavesdropping, also known as sniffing or spoofing, can be performed in the autonomous vehicles' keyless entry scheme [101]. VW group remote control, Alfa Romeo, Chevrolet, Peugeot, Lancia, Opel, Renault, Ford, and others affected the keyless entry systems of the car [20]. By dropping a single signal from the original remote control, an adversary may clone a remote control and gain unauthorized access to a vehicle. A correlation-based Hitag2 assault enabled them to clone a remote control over a laptop computer within a few minutes.

### F. SYBIL

Sybil attacks [79] usually are signified by jammed network systems when some fake nodes are integrated into the system. Thus, autonomous vehicles cannot convey data and fail to detect the attacks happening, which leads to accidents. Google's car was under Sybil attack [97] in 2018. Attackers used the routing table's flaws, and non-encrypted messages of Google car and fake nodes were used to send misleading location and traffic condition information to the Google car. For this Sybil attack, Google car was showing incorrect GPS location and caused the vehicle to stop in the middle of the road.

Table 4 shows the top 28 attacks out of the reported 126 attacks. The attacks on each unit and warning messages, as well as government strategies for preventing attacks on self-driving cars adopted by different countries, are presented in the following sections.

#### 1) ATTACKS ON INERTIAL MEASUREMENT UNIT

Along with GPS, Inertial Measurement Unit (IMU) is used for vehicle navigation (e.g., positioning, motion tracking). To this end, Zhao [102] showed how the advancement of telemetric systems could introduce an integrated and connected community and thus enhance the capability of a vehicle contributing to safe driving through ITSs and on-board entertainment. This is because automotive technology is rapidly advancing towards V2V and V2I connectivity. Such advancement and integration expose cars to potential threats. Early research by Wolf *et al.* [103] identified such threats when the ECUs were being interfaced with systems like Bluetooth, GSM, and GPS modules to receive updates.

For discovering the vulnerabilities in the IMU and wireless connectivity, attackers demonstrated how they took control of a Cherokee Jeep. In July 2015, two scientists, Charlie Miller and Chris Valasek, hacked into the Cherokee from Miller's basement when the car itself was ten miles off the highway [91]. They were able to remotely control car functions via a simple 3G connection that exploited a loophole in the Uconnect system. Uconnect is an Internet-connected software that controls the navigation and entertainment system of the vehicle. They also rewrote the adjacent chip firmware into the car's head unit through Uconnect's cellular connectivity loopholes and creating an entry point. Consequently, they were able to send instructions to suppress the brakes and gain control via the IMU. The driver of the car had no power over either the steering wheel or the pedals.

In the above two examples of ethical hacking, hackers controlled the vehicle as part of an experiment-cum-stunt to prove that vehicles can be hacked and even operated remotely. The reaction of the demonstrations resulted in a security alarm concerning over one million Fiat Chrysler cars. It also served as a wake-up call that highlighted the danger hackers might pose to the automotive industry [74].

It is noteworthy to state that hacking vehicle sensors ethically to simulate false yet realistic data will cause the control system to react. It can be foreseen that compromising a sensor that is directly associated with the vehicle's safety operation may result in severe malfunctioning. For example, simulating a vehicle that is currently on a steep gradient may force the vehicle to travel at a very low speed and make it uncontrollable by the driver or the safety system of the vehicle. This security infringement represents a Denial of Service (DoS) attack on an autonomous vehicle [71].

This type of DoS attack creates interference on the sensing data or intercepts transmission between Radar and the sensors. In these systems, regulation components keep the Radar data within their acceptable limit. On the other hand, authorizing a hacker to know the acceptable range of sensed values may permit the hacker to modify the activities of the autonomous vehicles without affecting the ECUs. These forms of attack put self-driven cars or, generally, any vehicle under a threat that can severely impact their functionality. From the previous illustration, wherein the inclinometer sensor of the steep ascending/descending car is compromised, the fast motion of the autonomous vehicle may cause fatal accidents of hit and run or even destroying other people's property. Attacks like these need a comprehensive understanding of communication systems among sensors fitted with vehicles. [126].

Tools like CarShark [115] were implemented to detect the movement of a system such as a Controller Area Network (CAN) vehicle system. Authors in [115] confirmed the movement detection functionality on similar bus networks using the Car Shark tool. This research involved carrying out a comprehensive study of data packets and their manipulation

**TABLE 4.** Recent attacks happened on self-driving cars. Note that these are the attacks that were demonstrated either on-road or at designated test sites.

| Name of the attack, Year | Manufacturer, lab or others | Exposed vulnerability | Impact | Type of Attacks | Mitigation approach adopted/ recommended | Violated security |
|---|---|---|---|---|---|---|
| Attacks on AV software [109], 2018 | Tesla | Software flaw (weak message propagation algorithm) | Sensitive information leakage cause | Malware: Inserted malware program to the AV using the OBD port | Suggested updating antivirus software and applying sandbox approach | Availability/ Authentication |
| Attack on OBU [110], 2018 | Lab | OBU vulnerability on Lane Change Unit | Unauthorised manipulation of routing table | Jamming: Jammed the GPS component of the car that caused incorrect lane change | Intelligent IDS using back Propagation neural networks to detect abnormal/malicious behaviours | Availability |
| Speed control of Tesla from outside [111], 2017 | Tesla | Hardware flaws of speed control sensor | Disclosure of sensitive information | Sensor impersonation | Central gateway-based architecture in the automotive bus system | Authentication |
| Google car hacked [112], 2016 | Google | OBU's component vulnerabilities and sensors malfunctions | Network flooding with wrong information | Bogus information | Encryption and obfuscation techniques to prevent code tampering and data sniffing | Authentication/ Integrity |
| Honda updating wrong car manual [113], 2017 | Honda | Insecure cryptographic algorithms | Vehicle software update system was unable to update the correct software that would affect the safe operation of the vehicle | Remote firmware | Secure Firmware updates Over The Air (FOTA) | Authentication |
| Attack on GPS [114] , 2016 | Tesla | Software flaws and weak password | Sensitive data leakage | Social engineering-based | Encrypted and strong password for message communication | Integrity/ Privacy |
| Jeep was remotely controlled by hackers [94], 2015 | Jeep | Ethical hackers accessed the vehicle remotely | Vehicle went off-road because of false/incorrect GPS data | Remote access | Encryption and obfuscation techniques to prevent code tampering and data sniffing | Authentication |
| Ignition auto start – Benz [115], 2018 | Mercedes | Wireless-enabled OBU vulnerabilities and thus insecure wireless communication | Revelation of user identity | Attack on privacy | Suggested implementing Secured Vehicle Communication (SeVeCom) [116] | Privacy/ Authentication |
| Broadcasting log file [95], 2018 | Honda | ECU vulnerabilities: broadcast nature of messages via wireless communication channel | Leakage of sensitive information and private credentials | Eaves- dropping | Strong encrypted message for wireless communications | Privacy/ Authentication |
| Attack on Lidar [117], [118], 2018 | Tesla | Wireless enabled OBU vulnerabilities and insecure wireless communication channel | Prevented vehicles from receiving sensitive information and using network services | Jamming | Assigning IPs to vehicles and dropping duplicate IP during message transfer. Changed Packet Delivery Ratio (PDR) based on PDR rate decrease. | Availability |

**TABLE 4.** *(Continued.)* **Recent attacks happened on self-driving cars. Note that these are the attacks that were demonstrated either on-road or at designated test sites.**

| | | | | | | |
|---|---|---|---|---|---|---|
| Attack on wireless enabled OBUs [119], 2017 | Lab | Insecure wireless communication channel | Messages alterations | Imperso- nation | Identity-based batch verification scheme | Authentication |
| Driver losing steering control [120], 2018 | Jeep | Plaintext messages and insecure wireless communication channel | Injected false messages | Man-in-the-middle (MITM) | Encrypt the data transmission between the external memory and the ECU internal memory on-the-fly | Availability/ Confidentiality |
| Incorrect road condition report, causing vehicle to stop [115], 2018 | Lab | Vulnerable wireless communication channels | Message manipulation and dropping | Spoofing | Multi-antenna system with known movements and in-region verification | Authentication |
| Incorrect GPS location [121], 2018 | Google Car | Flaws in routing table and non-encrypted messages | Data leakage on back-end wired channel | Sybil | Position verification of neighbouring nodes, VANET PKI [122] and RobSAD [123] | Authentication/ Availability |
| Unable to control brake [93], 2015 | Jeep | Hardware vulnerabilities | Message alterations en-route to other vehicles via RSU and CTC | MITM attacks between RSU and CTC | Strong cryptographic techniques | Confidentiality/ Availability |
| Attacks on ECU [45], [46], [124], 2010 | Lab | Vulnerable ECU software | Controlled vehicle components remotely by reprogramming ECU software | Remote access | Updated system software | Authentication |
| Attacks on UConnect system [47], [125], 2016 | Tesla | Security issues with third party software and vulnerable to data injection | Taking OBU operational control from driver or car remotely | Unauthorized access | Change firmware settings | Authentication / Data integrity |
| Malicious data to Controller Area Network (CAN) bus [126], [127], 2014 | Lab | Compromising security keys used by ECU | Several OBUs stopped functioning or started malfunctioning | Unauthorized remote access | Suggested Elliptic Curve Digital Signature Algorithm (ECDSA) to improve ECU security key | Availability/ Non-Reproduction |
| Attack on Mitsubishi Outlander [128], 2016 | Mitsubishi | Insecure messaging protocol | Turns lights on and off, disables anti-theft alarm | Man in the middle alarm | Update firmware and messaging software | Availability/ Confidentiality |
| Attack on Volkswagen keyless entry system [54], 2016 | Volkswagen | Global master key information retrieved from ECU | Able to gain unauthorized access to many Volkswagen cars | Eaves- dropping | Update master key information | Authentication/ Data Integrity |
| Attack on Nissan Leaf cars [76] , 2016 | Nissan | Vulnerable Nissan Connect application | For the software flaw, hackers could have recent journey information and drain out the battery of the car. | Unauthorized access | Suggested using secure firmware updates over the air (FOTA) to secure the in-vehicle applications | Availability/ Non-Reproduction |
| Attack on GPS - Offset insertions [83], 2019 , | Multiple | Vulnerable GPS location prediction | Vehicle GPS can misread its location by approximately 10 meters, which forces the vehicle to change lane, move left or right, go off-road, and make a sudden stop | Spoofing | Suggested using blocking antenna to protect against interference and jamming, and reduce the danger of spoofing signals. | Availability/ Authenticity |

**TABLE 4.** *(Continued.)* **Recent attacks happened on self-driving cars. Note that these are the attacks that were demonstrated either on-road or at designated test sites.**

| | | | | | | |
|---|---|---|---|---|---|---|
| Attack on GPS - Timing attack [82], 2019 | Multiple | The vulnerability of a vehicle's data transmission | The actual vehicle position was replayed to the GPS receiver but delayed by several seconds. The vehicle slowed down because of inaccurate on-road position | Jamming | Verify packet delay using Timing Attack Prevention protocol [129] | Availability |
| Attack on Camera image [130], 2018 | Simulation | Vulnerable image processing | Hackers were able to alter the images captured by the camera of the car | Unauthorized access | Suggested using multiple sensor input (e.g., multiple cameras, radar, Lidar) [131] | Availability/ Non-Reproduction |
| Attack on Controller Area Network (CAN) Protocol [132], 2017 | Simulation | Vulnerable messaging system in CAN | Overloaded the system with error messages and making the CAN system stopped working | DoS | Suggested using Identity-based batch verification scheme [133] to secure CAN messaging system | Authenticity/ Availability |
| Attack on On-Board Diagnostic (OBD) [134], 2018 | BMW | Vulnerable BMW OBD2 to malware | Hacker inserted malware to the OBD2 unit, and the diagnostic system of the vehicle failed to operate | Malware | BMW fixed bug in TCU and OBD in their vehicle operating system update [134] | Availability/ Non-Reproduction |
| Attack on central operating system [135], 2016 | Toyota | Vulnerable central operating system | Able to insert ransomware (WannaCry) to the operating system of the vehicle | Unauthorized access | Security patch of vehicle operating system updated. | Availability/ Non-Reproduction |

violating data integrity, like the simulation of a man-in-the-middle attack and detecting its impact on a vehicle. The experiments involved modern vehicles without self-driving functionality; still, the researchers were able to modify the packets containing Radar data during transmission. Recommended mitigation mechanisms to prevent such attacks are:

1) The use of encrypted messages on the vehicle's communication network. Since the encryption technique provides confidentiality and data integrity security services, this can ensure that counterfeit signals cannot be easily injected onto the network.
2) Rigorous monitoring of the signal behavior to make sure that it is within the expected range or behaving normally [23], [127].
3) The disposition of additional sensors (e.g., Light assist, lane assist, front assist) offers a secondary foundation of dimension. For instance, using the G.P.S. as well as plotting information can assist in determining if the autonomous vehicle is situated on sharp gradients.

Koscher *et al.* [115] demonstrated that an invader is capable of infiltrating virtually any ECU. The unit possibly will influence this capacity to evade a wide-ranging range of security systems entirely. It confirmed the ability to enforce hostile mechanisms above a comprehensive range of motorized tasks and entirely ignore motorist response together with inactivating the brakes, braking separate controls on request, and ending the car's motion.

Attacks on airbag control, ECU, and electric window lifter were demonstrated by Hoppe *et al.* [115]. San Diego's [45] team of researchers from Washington University and the University of California experimented with a multitude of attacks such as cd players, Bluetooth, and radio.

In 2016, a group of Keen Security researchers [46] took over the infotainment screens and instrument cluster displays and unlocked the doors of a Tesla X remotely. The trunk was also opened, a side mirror could be folded, and the brakes turned on while the car was in operation. The scientists could open the sunroof remotely, shift power seats and switch the signal lamps on.

### 2) ATTACKS ON LIDAR

Lidar technology is used to generate 3D maps of a vehicle environment for localization, obstacle avoidance, and navigation. Lidar measures the distance by measuring the flight time of a laser beam projecting vertically to the ground. This flight time is used to determine the presence of an object and its distance from the car. Self-driving cars are highly dependent on Lidar systems. As shown in Table 4, the Lidar of a Tesla's vehicle was under attack by hackers and unable to detect a van in front of that autonomous vehicle. As a consequence, this Tesla vehicle hit the van [128]. Researchers also tested for other possible attacks that can happen on Lidar.

Stottelaart *et al.* [129] showed by a lab experiment the likelihood of congestion because of an attack on Lidars by

leading the emanating light posterior to the scanner component, which has the same rate of recurrence as a laser replicating from the object [129]. Petit and Shladover [111] ethically hacked a self-driving car using a raspberry pi and thereby breached automatic, and net linked vehicles using their created cyber-attacks. They were capable of interfering with the Lidar structure to coax it into not sensing any highway obstructions like debris, people, cars, buildings, etc. This interference can lead an automatic or self-driving car when moving at maximum speed to stopover, and thereby inactivating the vehicle. For example, because of the car sensors receiving jamming signals from raspberry pi, a Lidar unit failed to notice any highway debris or people or obstructions during its right turn. Consequently, the car hit the obstacles and immediately stopped after traveling around a hundred meters.

Lidar plays an important role in the safe self-driving operation of a car. However, Lidar is yet to prove its effectiveness in preventing or detecting cyber-attacks. Modern Lidars use different wave intervals to thwart possible cyber-attacks and prevent attackers from creating jamming or congestion, in-between the Lidar pulse signals. Using these methods to prevent attacks can reduce the effectiveness of normal Lidar function in detecting objects [129]. There are other potential ways, including mitigation tools available in the V2V message systems, to enhance the capability to counter such attacks. The main loop-whole of using such tools is that they can cause the Lidar to incorrectly detect object dimension, and this inaccuracy of object perception can compromise a car's normal operation. Another mitigation strategy is to apply a random examination of Lidar signals. This random examination will allow vehicles to modify the time between skimming speeds and thus will hinder attackers' ability to access the systems [115].

#### 3) ATTACK ON GPS

With a precision level of one meter, GPS provides absolute position data. GPS is an open standard available in the public domain; however, coded signals are utilized in limited GPS systems such as GPS systems for the military. GPS units are usually programmed to use the strongest signal because this signal is probably more reliable in an ideal world. GPS is universal, and its architecture is transparent, but distorted signals made by malicious activities can easily be generated to annoy and block a GPS device (interference, spoofing) utilizing its known architecture.

GPS spoofing is a rather complicated process involving the generation of incorrect GPS signals to confuse GPS receptors. An attack by spoofing can, for example, start with the transmission of fake signals synchronized with the correct signals found at the target recipient. The attack increases the strength of the phishing signals, which progressively divert the position from the target. This sounds relatively straightforward in principle; however, the hardware required to generate realistic signals is a complicated operation. As hackers see increasingly potential benefits of GPS spoofing, the generation of simplified plugs and play controls will become a reality in the future. The public domain already holds a complete theory on how to spoof GPS attacks. For example, the literature on successful attacks on GPS has been published [136].

Currently, however, the literature only contains examples of "proof of concept" attacks. For example, students at Texas University in 2013 showed how false GPS signals could be generated, which overloaded GPS signals progressively and eventually deviated a superyacht from its actual path. The superyacht control then reacted by warning the crew of this path deviation to change the GPS signal and started correcting it by setting a new course. The device used for that attack was developed, and this GPS forgery was reported in the public literature, demonstrating that the generation of the fake GPS signal is easily possible [137].

GPS use is well integrated to a large scale transportation activities such as high-value vehicles or vehicles carrying goods or heavy machinery. Since GPS has been developed as an open standard technology, research has been carried out to develop GPS counterfeiting measures. Numerous simple validation mechanisms can be implemented to prevent spoofing attacks. Monitoring identification codes, satellite signals, and time slots may help to detect spoofing attempts. O'Hanlon *et al.* [138] explained in detail how approximately 163 decibels of signal strength can be observed. A GPS simulator, such as the one developed by Humphreys *et al.* [139], could provide higher several magnitude orders of signal strength than the signal strength of any satellite on Earth's surface. GPS signals can also be monitored to check whether their relative change is within a threshold. O'Hanlon *et al.* [115] also suggested monitoring GPS signals to verify that its strength varies according to expectations and that they are not perfect. However, if an attack is sufficiently sophisticated to appear as authentic, the validation tests will fail, and the GPS device will be taken over without the vehicle ECU being aware of it. It is widely accepted that the strongest countermeasure to spoofing is the use of military-level encryption [139].

#### 4) ATTACK ON WARNING MESSAGES

It is essential to make sure that the safety of Vehicle to Vehicle messages, particularly data legitimacy and dependability due to the messages' nature exchanges in V2V communication (for example, acceleration, velocity, and position) because they are safety-critical. To ensure that the data content's legality is ambiguous and it is not possible to do it traditionally, although source authenticity message veracity can be guarded by cryptographic means. Harsh effects will include undermining the advantages of V2V communications if false data is received from another car. A dangerous circumstance can occur. For example, crashing accidents from the rear end can occur if, for instance, recent studies [140], [141] prove that in a CACC setting, feeding false data to a wireless conduit can cause a malevolent car to increase or reduce the speed of other vehicles incorrectly.

It is imperative to make sure that cars sense and filter data from other motor vehicles, given that a linked car's

**TABLE 5.** Possible and current attacks.

| Name of Attack | Attacker Type | Security Attributes or Requirements |
|---|---|---|
| Bogus Information [89] | Insider | Data integrity and authentication |
| Denial of Service (DoS) [141] | Malicious, insider, active, network attack | Availability |
| Masquerading [142] | Active, insider | Authentication |
| Black hole [84] | Passive, outsider | Availability |
| Malware [44] | Malicious, insider | Availability |
| Spamming [67] | Malicious, insider | Availability |
| Timing attack [84] | Malicious, insider | Data integrity, Authenticity |
| GPS Spoofing [90] | Outsider | Authentication |
| Man-in-the- Middle [143] | Insider, attack monitoring | Data integrity and confidentiality |
| Sybil [144] | Insider, attack network | Authentication |
| Wormhole Tunneling [145] | Outsider, malicious, monitoring attack | Authentication and confidentiality |
| Illusion Attack [87] | Insider, malicious | Authentication |
| Purposeful attack [88] | Active, insiders | Authentication |
| Impersonation [146] | Insider | Authentication |

decision-making process much depends on the received V2V messages. When drafting a trust framework for secure V2V data authentication, many challenges are present. Cars should be able to detect false messages and approximate the true states in real-time as the attackers may feed incorrect data from another car at any given time. Detection of untruthful data should be done in a manner that is confined and decentralized as a substitute for depending on national infrastructures to gather universal information such as the trusted roadside components. With the number of surrounding vehicles being small and the possibility of collusion, we cannot presuppose a candid, more significant part of the one-hop area of a car. To sum it up, since not all cars are fitted with highly developed detectors like radars, which are costly, the solutions are going to cost less. In VANETs traditional trust framework cannot gratify the suitable requirement without responding to every message in real-time since they are only needed to assess the long-term trust of the other fellow vehicles. A Mitsubishi Outlander PHEV was hacked, and the investigators of safety at Pentest Partners executed a man in the middle attack to know the one responsible between the PHEV's cell phone application and the Plug-in Hybrid Electric Vehicle (HEC) Wi-Fi application [118]. They were able to find out the binary protocol that was used for messaging after repeating the different messages from the mobile app. The attackers were able to switch on and off the lights, immobilize the entire burglary alarm system, thus making the car at risk of more attacks.

#### 5) ATTACK ON THRUSTER MONITORING UNIT

A self-driving car's thrusters, a type of propelling unit acting as actuators, are responsible for the faults or failures associated with different types of motions. The status of thrusters is monitored by a special unit called the Thruster Monitoring Unit (TMU). If this unit is attacked in a self-driving car, it can result in disturbances in the vehicle's fault control. The attack eventually takes control of the motion of the car. A self-driving vehicle will hardly have enough time to notify the driver to control the car in the event of such an attack. Very little research has been conducted on such attacks. Literature available on safety measures for controlling and preventing such attacks is minimal. Ironically, there is a comprehensive volume of poetry available in the public domain on how to carry out such attacks. It's an indication of the almost non-existent cyber controls and regulations regarding the same. Could it be a lack of goodwill by legislators and the systems in place? Test drivers for google driverless cars have a bit of leverage. They are trained on the car's technology and how to take control of the vehicle in case a situation needing that arises.

Drivers with little knowledge on the same will find it difficult to take control of a driverless car if a situation requires. Most tend to ignore safety procedures and implications associated with driverless cars. They are unable to decode the status of the control system when they have to take charge of the vehicle. Examples of such situations are when there are mode errors, system attacks, or the automation period lapses. In the event of the detection of a cyber-attack on a driverless vehicle, the driver needs to be notified. Notifying the driver and in good time will allow them to make informed safe decisions. Research on details of how a vehicle or driver should react if faced with a cyber-attack is lacking or scanty. Does the car have an automatic safe mode that ensures it is safely controlled? How does a vehicle detect it has been attacked and swiftly pass on this message to the driver? How will the car process detailed information in the case of an attack to enable the driver to make an informed and timely decision? All these questions need to be answered for a breakthrough in the safety of driverless cars against cyber-attacks [142].

#### 6) ATTACK ON AU

AU comprises many important applications (e.g., remote vehicle diagnostic applications). Therefore, an attack on AU can lead to exploiting the vulnerabilities in those applications installed in a self-driving car. Mostly, password and key attacks are reported on AU [143]–[145].

Application constraint structures are actively checked in the password and key attacks using various values to check if they are compromisable. These attacks can typically be classified into three key categories:

- dictionary,
- brute force, and
- rainbow table attacks.

A dictionary-based attack utilizes a comprehensive list of words that are available in a dictionary. These can be used individually or as a combination of words. They are repeatedly used to try and obtain the right password. A brute force attack has a bit of similarity to the dictionary-based attack. It utilizes a range of alphanumeric combinations. All of these words cannot be found in a dictionary. This category can be slow since the possible number of combinations is huge, almost infinite. However, the correct combination eventually works, revealing the password. The easiest way to use a brute force attack is on a Bluetooth pin of the car. This is because Bluetooth usually has a pin with just four digits, and thus, in the worst case, an attacker needs to attempt ${}^{10}P_4 = \frac{10!}{(10-4)!} = 5,040$ tries, which can be cracked in just seconds. Most attacks in this category are designed for compromising VANETs.

A rainbow attack has some similarity to the brute force attack and utilizes precomputed hashes. These hashes are listed in a table and generated from an algorithm that creates all the possible passwords. The use of a hash table gives a significant reduction in the time used to crack a password. An example of such an attack is that of Garcia *et al.* [146], who cracked a crypto algorithm popular with vehicle manufacturers. The algorithm was the 96-bit Megamos and took less than a week to build the hash table of 1.5 Terabytes size. However, an exhaustive search can be completed within seconds. This attack shows that the security mechanisms of vehicles are very vulnerable to security breaches and attacks. Such attacks include vehicle theft, now a great headache for vehicle owners and manufacturers.

Rainbow table attack requires specialized hardware and software equipment to implement successfully and sophisticated techniques to perform, but still a real threat. Most attacks in this category are motivated by financial gains and can be avoided by installing more secure keys and using robust encryption algorithms. However, as the risk is always present, one needs to regularly update the vehicle security features. It is also noteworthy that the ever-advancing technology, security features, and encryption technologies that are highly rated today will be easily cracked and less effective in the future. A vehicle is a long-term commodity with an expected long-lasting life, and the computing power and hardware available to hackers also progress day by day. With these concurrent situations, it is fair to articulate that the cryptographic features installed in a vehicle today will not guarantee protection for its entire life span. It places a dilemma in the hands of cybersecurity experts and vehicle manufacturers. However, there is hope for a lasting solution, owing to the increased technological advancements in both sectors [147]–[149].

So far, we have presented the attacks that were previously happened on the different OBU components of a self-driving car and the relevant countermeasures that were adopted or can be adopted to protect the self-driving cars from those attacks. However, for preventing the attacks on AVs, many countries have already introduced some policies or laws deal with security issues legally. These policies or laws are presented in the following section.

#### 7) GOVERNMENT INITIATIVES AND PROJECTS TOWARDS SECURITY GUIDELINES

Governments in various countries have taken initiatives to formulate policy guidelines and strategies to ensure the safety of self-driving cars and VANET in general. These initiatives are categorized continent-wise and described below.

In 2012, the USA road and transport authority founded a special department named NHTA to explore the wellbeing, security, and unwavering quality of perplexing and interconnected electronic vehicle frameworks [17]. This department proposed non-compulsory suggestions for improving the safety of vehicle gadgets and network protection of the electronic vehicles' autonomous function. In 2016, the USA also presented the SPY Car Act to address vehicle network safety hazards. The law contains arrangements to form preparations against the cyber-attack on AVs, as an example, demanding infiltration testing to assess AVs' strength to prevent cyber-attack and isolating necessary and basic programming frameworks integrate into the autonomous cars. This Spy Car Act gives determinations to guaranteeing the safety of the data gathered from internal or external communications [13]. This Act expects AVs to own the capacity to spot, forestall, and report endeavors at seizing the control of cars, even as catching the put-away information. Agreeing with the perpetual guideline of February 2018, AV producers have to guarantee AVs' capacity to spot and answer digital assaults as per the "proper and relevant" industry principles. The assignment of additional obligation to the department protects an AV's ECUs from unapproved access or utilizes and secures the respectability of the knowledge [150]. In 2017, Texas approved another Cybersecurity Act that educates the formation of a panel to analyze network issues of safety and also the "data security plans " of the organizations. The legislature of Michigan likewise proposed making a network protection board to prescribe network safety upgrades to state foundation and to tell apart approaches to enhance the state's online protection industry [14].

The EU embraced an assortment of systems to oversee network safety hazards in 2016 [18]. The EU authorized the enactment of online protection: "the Directive on protecting organization and data frameworks" (NIS order). This order delivered best practices rules for the web protection of associated cars, including both ordinary and AVs, to create attention to and provides direction on these issues. China introduced a way to handle the net protection dangers of all digital frameworks. China's new network safety law, introduced in June 2017, sketches out explicit arrangements to strengthen the safety of the communication network and individual data. This law enforces the obligations of organization administrators, controlling the offer of online protection gear, and laying out punishments for potential infringement. Organization administrators are needed to maintain security techniques to "defend networks from impedance,

pulverization, or unapproved access.'' These requirements profile how unacquainted organizations monitor information with additionally distributed ''Measures for Security Assessment of non-public Information and Important Data Leaving the Country.'' Growing the prerequisites for information localization to any or all arrange administrators, which can affect the makers of AV, hoping to check and convey their items in China [15]. Numerous arrangements of the law have all the earmarks of being intended to make sure public interests. For instance, the law accentuates on guaranteeing the safety of data moving at some stage in China and reliably assesses the protection of basic data foundation that is crucial for the general public enthusiasm even as the general public economy and peace [15]. The law likewise requires sensitive data to be protected within the nation, even though the legislature still can not seem to unequivocally explain what varieties of data they respect to be ''Sensitive.''

In 2017, Singapore received a broadened thanks to house overseeing network safety chances by correcting enactment, counseling various partners, and teaching the overall population about such dangers. The Act makes it illicit for people to utilize individual data ''got unlawfully from a PC'' and to accumulate ''hacking instruments'' to perpetrate or encourage violations [151]. The legislature introduced how to fortify the reaction to such dangers and limit the impact related to these dangers. Furthermore, exemptions are made if the influenced people are the topics of a ''progressing or likely examination under the law,'' and the assortment is encoded [151]. Generally, the Personal Data Protection Council (PDPC's) [16] proposed changes shall adjust the necessity for utilizing information with people's privileges to security assurance. Then again, the administrations of Japan and South Korea haven't given any sign of their thanks to pandering the overseeing network safety chances akin to AVs or digital frameworks tired all.

The Korean government changed the car Management Act in 2017. Notwithstanding, the law does exclude any arrangements for online protection. The law expresses that someone who wants to use data received from a car requiring the board of that car must acquire endorsement from the Minister of Land, Transport, and Maritime Affairs [12]. However, this law allows users to transmit or share data (speed of the vehicle, location without user information) that does not breach the privacy of the user. Additionally, Japan has not corrected enactment or given rules on tending to network safety chances as a rule or those who are explicit to AVs. While legislatures of Germany, France, Australia, and therefore the UK have not altered or presented any new enactment on network safety, they need to find a way on how to expand the consciousness of AV-related online protection chances. The German government started working on AV-related issues in September 2015, which incorporates network safety and data security as a component of its general procedure for ''Computerized and Connected Driving'' [10]. Similarly, the French government founded working gatherings in 2016 to handle AV-related cultural issues, one amongst which has security issues. As referenced within the Privacy segment, in Australia, the House of Representatives Standing Committee on Industry, Innovation, Science, and Resources (HRSCIISR) suggested coordination of the endeavors of assorted partners through the production of a public body [11].

Based on the recent attacks described in this section, the following section presents the countermeasures that have been taken or need to be taken for the types of attacks that happened or could happen in the future on self-driving cars.

## VI. OTHER POSSIBLE ATTACKS ON ITS AND COUNTERMEASURES

In today's vehicles, software-based ECUs have put almost every mechanical steering feature and have made it possible to make a huge save inconvenience and cost performance. ECUs are networked and exchange data, allowing extensive communications and regulations across one or more networks. The above also covers potentially important protection ADAS, for instance, the Adaptive Cruise Control (ACC) and the automatic parking or exit warning for lanes. Self-driving vehicles are assisted by an immense amount of complex programming, including routine operation ( e.g., braking, gear adjustments, acceleration), more complicated tasks (e.g., avoiding accidents), and general internal vehicle condition monitoring [152], [153]. Such complex systems increase the likelihood of software vulnerabilities that could impact the safety and health of the entire vehicle.

With regular software updates and enhancements, one can ensure the systems' correctness, efficiency, and reliability over the complete lifetime of the vehicle. As apps, ECUs, sensors, and microprocessors are increasingly dependent on self-driving vehicles, developers have introduced a high-performing combination of telecom processors, assisted by a robust Over-the-Air ( OTA) solution for device updating and data management. Some firms, such as Airbiquity and Renesas, incorporate Airbiquity's OTAmatic software and data management technology into the Renesas R-Car H3 automotive computing platform that serves as in-vehicle System-on-Chip (SoC) processors for powerful, safe, and unified communications ECU software updates and data management.

Over-the-air software updates and data management, wireless communications, and complex programming and functions have made self-driving cars susceptible to various types of cyber-attacks. As mentioned in the previous section, some of them have already happened. However, some are regarded as potential attacks exposing dangerous threats. Many types of possible and current attacks on ITS and VANETs considering the importance and aspect of different security requirements (e.g., availability, authenticity, integrity, confidentiality, accountability) and privacy issues along with attack mechanisms and mitigation approaches (refer to Table 3) are discussed in the following sections.

**TABLE 6. Summary of possible and simulated Attacks on Autonomous Vehicles and ITS.**

| Target | Attack Type | Impact | Described in |
|---|---|---|---|
| Infrastructure | DOS attack | Attackers can carry out a Dos attack on a roadside unit which can delay a road emergency message. | S. Erskine and K. Elleithy [165] |
| | Passcode attack (internal network) | Attackers can hack connected cars and compromise the user's privacy. | Parkinson et al. [166] |
| | Vehicle to infrastructure attacks (integrity) | Attackers can manipulate the smart traffic signals and nodes to disrupt the traffic flow and cause accidents. | Parkinson et al. [166] |
| | Vehicle to infrastructure attacks (availability) | Attackers can withhold important information such as intersection congestion and obstacle detection to cause accidents. | Islam et al. [167] |
| Vehicle | Automated system hijack (auto-pilot mode on) | The car was hijacked, and pedestrian life was compromised as a result. | Elliot et al. [168] |
| | Automated car hijack (auto-pilot mode off) | The car can be forced to stop unexpectedly resulting in a roadblock or an accident. | Linkov et al. [169] |
| | Car spoofing | Attacker pretending to be a neighboring car can send false data to the car resulting in an accident. | Linkov et al. [169] |
| | Compromising the keyless lock system | Attacker can keep a person locked inside a car. | Hussain et al. [170] |
| Camera | Information modification (using infrared light) | The camera was used to send a command through infrared signals to open the gate of a facility. | Guri et al. [171] |
| | Physical integrity attack | An attacker can change the physical configuration of the camera to cause an accident | Sheehan et al. [172] |
| | Camera Spoofing (advanced driver assistance systems) | ADAS systems were introduced to alert drivers and control the vehicle to prevent accidents. An attacker can spoof the camera and fool the system into causing an accident. | Costin [173] |
| | Man-in-the-middle | An attacker can get video surveillance footage, and an accident happened. | Cusack et al. [174] |
| Radar | Spoofing attack | The attacker confuses the radar by giving false signals due to which it does not detect its surroundings. | Raiyn [175] |
| | Physical integrity attack | An attacker can use absorbent objects to confuse the sensor into believing there is no obstacle at the front and cause an accident. | Sheehan et al. [172] |
| | Replay attacks | An attacker can send any old packet to the sensor to generate a false output which may cause a disturbance in traffic flow. | Hussain et al. [170] |
| GPS system | GPS spoofing | The attacker can provide the wrong directions and mislead the car. | Sheehan et al. [172] |
| | GPS jamming | The attacker can control the route of the vehicle and endanger passenger life. | Sheehan et al. [172] |
| | GPS tracking | An attacker can track the location of a target. | Parkinson et al. [166] |
| | Man in the middle attack | An attacker can become a man in the middle and access the location, manipulate it and carry out malicious tasks. | Raiyn [175] |
| In-Vehicle devices (e.g., multimedia systems) | Passive attack | An attacker can observe the target's routine. | Parkinson et al. [166] |
| | Man in the middle attack | An attacker can infect the system with malware to cause the in-vehicle devices to malfunction. | Raiyn [175] |
| | Spoofing | The attacker can choose what to display on a screen or what to play on speakers and can blackmail the target. | Hussain et al. [170] |

### A. ATTACKS ON AVAILABILITY AND COUNTERMEASURES

The accessibility of ITS systems is set to make sure that the security of passengers and autonomous vehicles is enhanced. From this framework, DoS spasms, i.e., renunciation of the provision, are currently acknowledged as the entire unsafe risk to the accessibility of systems of ITS since their significant effect is on the convenience of the system resources. The key objective of the attacks is to inhibit ITS unit's uses and autonomous vehicles from exhausting network facilities in addition to supporting. This attack can be apprehended in the system by core or mischievous peripheral nodes. Additionally, disseminated Distributed Denial of Service (DDoS) attacks are even further destructive. The next topic has numerous examples of intended DoS as well as DDoS attacks, e.g., jamming, etc. and their equivalent countermeasures [164].

In March 2018, during the test drive of an Uber's auto taxi service, a hacker took control of the vehicle and logged into the system with a different user name. The auto taxi failed to collect the passenger from the designated area as the hacker sent the car in a different direction. Attacks [69], [90], [104], [110], [113] shown in Table 4 represent the attacks on availability.

- Jamming attacks: These types of attacks are realized at the corporal level, and they aim to interrupt the

communication network by conveying noisy signs to upsurge the intervention level. It leads to fewer Signals to Noise Ratio (SNR) and causes the autonomous vehicles to be incapable of communicating with others as well as RSU Stations. The impacts of jamming may be sensed and moderated with detailed methods, for instance, by actualizing the rate of recurrence through Frequency Hopping Spread Spectrum (FHSS) tools using intelligent pseudorandom creator algorithms in orthogonal Frequency-Division Multiplexing (OFDM) standards [165], [166].

- Flooding attacks: Most of these attacks are those that flood systems of communication with spasm messages, which are usually generated through some mischievous nodes. These messages tamper with communication channels between the RSUs and OBUs' wireless communication channels. It results in some fatal accidents occurring when the security of communication is compromised, and the vehicles cannot channel communication between themselves [84].
- Sybil attacks: Different ways can be used to protect drivers and passengers from Sybil attacks. They include the Central Validation Authority (CVA), used to accept validated units. The validations procedure is either indirect or direct. In complicated processes, any inward bound node must prove itself using the CVA. By creating an uninterrupted connection, whereas the direct facilitates the CVA. to receive a readily logical entity. Credentials used via the CVA.s are usually transitory. Additionally, the verification process is further reinforced by the remoteness bounding conventions, e.g., bit commitment as well as the zero-knowledge techniques. Specific decisions for Sybil attacks include unidentified nodes authentication through secure location encryption [69]. Other solutions to Sybil attacks comprise validating unknown nodes with the means of secure location verification [167], [168].
- Malware attacks: These are the ones that use worms, viruses, as well as Trojan horses to affect the autonomous vehicle's network. They also affect the software constituents of the RSUs and OBUs. These attacks lead to hazardous magnitudes of ITS structures, and these may be moderated using antimalware kinds of software. Conversely, new polymorphic malware types may alter their form and dimension, whereas metamorphic kinds of malware also adjust behaviors through the duplication phase, and this complicates detection capacities. The distinctive cryptographic measure comprises of validation of software updates as well as authenticating them in advance to their installation [169].
- Spam attacks: The fundamental goal of these attacks is to devour the system bandwidth hence vastly increase the invisibility of a system by transferring spam communications to users. The regulation of spamming emails is challenging due to the deficiency of consolidated infrastructure. [87].
- Blackhole attacks: such attacks can be present in several kinds of ad hoc systems, comprising ITS, and they are considered as frequent attacks against accessibility. Blackhole attacks are designed within a system when malevolent nodes decline to transmit messages. The Blackhole attacks mean that an evil node designates its active involvement in the interior of the system, but it doesn't usually take part. These Black hole attacks are very unsafe for numerous applications of ITS, particularly for sensitive highway security applications [87].

#### 1) ATTACKS ON AUTHENTICITY AND COUNTERMEASURES

Authenticity is an essential requisite in ITS structures to certify the safety of valid nodes alongside numerous attacks, comprising black holes, and reiterate attacks. This digital sign denotes the utmost frequently used cryptographic measures for verifying the validation of ITS units. It permits receivers to authenticate the source of information. Simply the legitimate nodes have the right to use the resources and facilities of ITS. Any fault in the procedure of documentation or verification can render the whole network susceptible to unembellished consequences. Without a doubt, both exterior and interior attacks come about via fake identities. More information on the sampled of counterfeit entities is explained below. These include; fraudulent entities along with other equivalent cryptographic measures [69], [77], [90], [92], [105]–[108], [112], [113] shown in Table 4 are the attacks on authenticity.

- Falsified entities attacks: In forged units' attacks, the attacker acquires a legal identifier and licenses to another valid node, establishing a degradation of the verification procedure. Each ITS unit has a system identifier that allows differentiating it from other ITS system nodes. For instance, rogue APs admittance points may be positioned along the wayside to imitate valid RSUs as well as to inaugurate attacks taking place in the connected users and autonomous vehicles, as presented in [20] of Table 4. Falsified entities' attacks may be prohibited by executing proper verification mechanism. For instance, using the standard primary encryption method, where all ITS units are connected with legal digital documentation, contracted by the ITS expert witnesses.
- Cryptographic replication attacks: In Cryptographic replication types of attack, sources or arithmetical documentations are replicated to generate opacity. Such vagueness can inhibit the ruling classes from recognizing an SC, particularly in the situation of an argument presented in [88] of Table 4. The commended measures against these occurrences are frequently using licensed and nonrefundable sources to fight the attacks. The verification of the license validity through a Certificate Revocation List (CRL)or an authorization cancellation list is an alternative solution. On the other hand, the second resolution is perplexing in the framework of ITS, as it needs cross accreditation trusts amongst the diverse

certification establishments involved in the security system of ITS.

- GNSS spoofing and injection attacks: When it comes to ITS, location data is of vital significance, and it needs to be precise and reliable. Such information is usually acquired from the GNSS. From this perspective, GNSS hoaxing and inoculation attacks are well-thought-out to be the utmost risky hazard to supportive ITS. These GNSS spoofing and injection attacks provide nearby self-driving cars with deceitful location data. The precise location data is usually acquired from a GPS scheme like the one that was launched in the U.S.A. with the integration of GPS receivers. This type of attack was propelled using a receiver producing localization indicators resilient than those created by the actual GPS satellite broadcasting (see man-in-the-middle [132] presented in Table 4). A prosperous GPS satirizing attack can enable other occurrences, such as spasms against setting based proof of identity approaches. This occurrence can be prohibited using sign systems with location schemes that agree to take only certain location information.
- Timing attacks: When it comes to ITS security applications, the appropriate conveyance/reaction of secure communications is of crucial significance to guarantee the security of drivers as well as passengers [112]. In this framework, timing attack interrupts the conveyance of delicate delay communications; hence the security necessities are not accomplished in time. This Timing attack type forces authentic ITS units to convey their communications through mischievous node/shafts, which interrupts the reaction of these communications by other valid groups. The standard measure is to increase the time imprints to the delay delicate packets. Still, this measure needs more multifaceted time management [133].

### 2) ATTACKS ON DATA INTEGRITY AND COUNTERMEASURES

The purpose of integrity protection is to guarantee that the substituted communications are not transformed all through their conveyance by a malevolent user. Additionally, information integrity provides the capacity to fight damage and the illegal establishment of information. A valid node in a system can be susceptible to exterior and interior attacks. The end product of exterior attacks is generally less equated with that of internal aggression. The second also contributes to giving attackers uninterrupted hardware right to use. Attacks [106], [108] shown in Table 4 are the attacks on Integrity. For data integrity, cryptographic hash functions are the necessary solution, and a signed hash authenticates a legitimate sender of the message.

Some examples of attacks on data integrity are briefly listed in the following.

- Masquerading attacks: a malevolent node customs a true identity of additional nodes to make sure that it has the form of a positive note in this type of attack. Attackers try to create deceitful communications and transmit them to the nearby self-driving cars to achieve precise intentions, for instance, to deliberate decrease the quickness of a car. A malicious node tries to perform as an alternative car and therefore tricks other self-driving cars to maintain a clear way or provide the means. To prohibit this attack, a CRL license cancellation list is used to preserve the characteristics of the identified malicious cars, which is then dispersed to all nodes in the ITS system. Although this resolution can moderate the impacts of the concealed attack, it needs the enactment of the effective malevolent nodes recognition system. [134].
- Data playback attacks: A replay attack replays a formerly transmitted communication. An information playback attack usually manipulates self-driving cars' settings as well as their course-plotting tables. Also, to protect sensitive information against attacks, a cache may be instigated on OBUs as well as RSUs. The cache will equate the freshly received communications with the ones from the past to discard the replicated messages. Additionally, a safe and sound session demonstration may be created to detect a message session amongst two units distinctively. Nonce an unsystematic digit used one time in cryptographic schemes may also be subjugated to guarantee that each communication is handled only one time [85].
- Data alteration attacks: An attacker falsifies attacker forges received communications to attain the voluntary benefits through leading the car owner to alter the verdict, such as designating a specified route that is overcrowded or not. An additional hazardous risk is the injection of deceitful security messages hence impacting the security of motorists and cars. Numerous systems Vehicular Public Key Infrastructure (VPKI), vehicular open essential structure, zero-knowledge) are involved in terminating this risk and making sure the verification amongst cars and substituted ITS communications is enabled. An additional efficient technique that launches group messages, where the sources can be accomplished by a collection of vital administration, is the Group Key Management (GKM) system. In this technique, an impostor cannot converse with the group participants [86].
- Map catalog poisoning attacks: Centered on the substituted communications (e.g., transmission safety communications), every OBU forms and conserves an indigenous map catalog to hold onto the track of all nearby self-driving cars, actions, and topics of concern. Map catalog poisoning attacks send mischievous communications to the indigenous map catalogs of ITS units hence letdowns the security of ITS uses and operators. The necessary countermeasure encompasses validating the signs of the acknowledged communications, distinguishing, and debarring the mischievous nodes [135].
- Data tampering attacks: Data tampering attacks can be recognized by valid nodes, which can terminate the

system, and risky root significance, such as mishaps, by formulating and dissemination of false communications. Its setup comprises hiding the genuine, secure connections to authentic operators and attempts to create and add forged safety alert emails in the system. A remarkable measure is to signal and validate the conveyed interactions. An enhanced setup is also necessary to identify the attacker's distinctiveness, which has to be added to CRLs [20].

#### 3) ATTACKS ON CONFIDENTIALITY AND COUNTERMEASURES

The concealment of ITS communications is necessary for some precise applications, for instance, to offer secure tax expenses as well as Internet facilities by encoding the communications transmitted amongst self-driving cars and RSUs. But, if the substituted connections do not have any delicate data (e.g., ITS security message transmission), concealment is not essential. Several attacks can have an impact on the system throughout the absenteeism of discretion safety mechanisms. Attacks [167], [170] shown in Table 4 are the attacks on confidentiality. In the following, some examples of these attacks, such as eavesdropping and data interception on ITS, are identified along with their countermeasures.

- Eavesdropping attacks: This attack has an impact on system privacy and does not influence system resources as well as accessibility [90], [171]. This type of attack allows an attacker to excerpt sensitive data from the communicated packages, such as the position data of self-driving cars. To offer resistance counter to these types of attack, all delicate files that have vital significance is to be encoded to make sure that the critical data of ITS units and their email are not disclosed [172].
- Data interception attacks: This attack has an impact on data privacy. Hence this is a risky attack. In Information interference attacks, an antagonist eavesdrops on the system for a precise time. Then he/she attempts to examine the composed traffic to excerpt the determined amount of valuable data. Similar measures that propose fighting eavesdropping can be implemented to safeguard from road traffic study attacks [173].

#### 4) ATTACKS ON NONREPUDIATION AND COUNTERMEASURES

Nonrepudiation safeguards against deceitful denials of involvement in a communiqué occasion and offers the receiver with evidence that the dispatcher is held responsible for the produced or wrought communications. The critical objective of nonrepudiation is gathering, retaining, creating accessibility, and authenticating undeniable proof about an occurrence or act. Nonrepudiation can be influenced by verification, but it produces a piece of firm evidence, as the structure can recognize the attackers or mischievous operators. They cannot refute their offenses or activities. Any carriage data (e.g., speed, journey route, damage) is kept in a Tamper-Proof Device (TPD), and an approved official can recover this data. Currently, we have offered potential attacks on self-driving cars, ITS, RSU, or VANETs for safety breaches, as well as their recommended mitigation methods. Conversely, confidentiality is a vital matter in an ITS scheme; the subsequent sector presents the attacks on the privacy of an ITS structure and its measures [174], [175].

Up to now, we have presented possible attacks on self-driving cars, ITS, RSU, or VANETs for security breaches and their suggested mitigation approaches. However, since privacy is a crucial issue in an ITS system, the following section presents the attacks on the privacy of an ITS system and its countermeasures.

#### 5) ATTACKS ON PRIVACY AND COUNTERMEASURES

The confidentiality of ITS units and their communications is a crucial necessity, and all delicate data are to be secure, comprising the identities of the car owners, their driving performances, and the past vehicle positions. Still, specific ITS highway security applications need the conveyance of entity-centric information (e.g., location, speed, and heading) to inform the nearby self-driving cars and infrastructures about possible road risks. Additionally, when a dispute arises (e.g., mishaps, highway traffic crime, mischievous users), the ITS structure operatives must recognize the identities of the connected drivers and cars involved in the problems. There is consequently a vibrant tradeoff amongst the confidentiality and safety requirements.

Zhang *et al.* [89] some attacks on confidentiality on ITS or VANETs. An example of an attack on privacy in ITS is tracing the cars and their drivers throughout the trips. Certainly, ITS units are customarily fitted out with Wi-Fi or Bluetooth aided devices, which transmits many facts in the vibrant text (e.g., identifiers, MAC, speeches, devices categories). This data can be composed by a third party to triangulate the locations of motorists and trail their drive within a metropolitan setting. The broadly used and commended measure is to use randomized or momentary identifiers (e.g., MAC and IP speeches) to detach them from the self-driving cars and their motorists. An additional method was presented by manipulating pseudonyms to make sure unidentified communications are controlled [43], [176].

## VII. RESILIENT OPERATION OF SELF-DRIVING CARS UNDER CYBER-ATTACKS

While the previous section reports the possible cybersecurity holes in the ITS system and in AVs that leads to attack and the ways to prevent such attacks by tightening the security mechanism, this section presents the current research trends that want to ensure safe operations of self-driving cars even under cyber-attacks.

In [24], Matthew *et al.* model and detect a replay attack, where an attacker replays a previous measurement to the system. They used a Linear Time-Varying (LTV) system

with an added dynamic private excitement to the input signals called dynamic watermarking to detect replays attack. The proposed LTV system extension allows several steps-gap from a control input signal being taken to its effect to be seen in the measurement signal and still can ensure the asymptotic guarantee of attack detection infinite time, which makes their model applicable for autonomous driving with more complex motions such as lane changes, turns, and changes in velocity. Furthermore, an introduction of the auto-correlation normalizing factor in the LTV ensures the practical, implementable statistical test can yield consistent results by removing residual anomalies present in a signal measurement. Dynamic watermarking is also utilized in [177] to secure an AV from arbitrary sensor attacks on adaptive cruise control systems.

Raghu *et al.* [25] proposed a 3-dimensional quantization index modulation (3D-QIM) based data-hiding model that can detect Lidar point cloud data tempered with either an inserted fake object or a deleted target object. The model can detect and localize data tampering attacks while data is transferred from the sensor to the ADAS unit for decision making, thus ensuring a data integrity verification for the autonomous vehicles. Using 3D-QIM, a watermark is embedded into the 3D Lidar point cloud data (also known as information hiding) using a quantization pattern, while the ADAS extracts the embedded signals by applying the same quantization step-size and pattern, and any difference between embedded and extracted message signals a data tampering. In [178], the authors modeled the Lidar spoofing attack where the attacker injects fake LiDAR data points by shooting lasers to present an obstacle close to the attacked vehicle. The attack model is successfully applied to produce (i) emergency brake attack and (ii) AV freezing attack. Similarly, in [179], attackers inject a phantom, a depthless object projected by special tools, intended at causing ADASs systems to perceive the inserted objects and road signs as real and force the ADAS to take unrealistic actions. Convolution neural networks are trained to determine the contexts of the inserted objects to mitigate the impact of such a phantom attack.

Vehicle platooning is a very important application of AVs and ITS, where a series of vehicles follow each other at constant speed and distance while receiving the controlling signals from the very first vehicle (leader). Several attacks are possible to disrupt such vehicle platooning, especially using GPS spoofing and replay attacks. Considerable efforts are underway by the researcher to ensure the smooth operation of such a system under various attacks. In [27], Xingkang *et al.* proposed a secure distributed algorithm for a platoon of autonomous vehicles, which can detect and mitigate an attack on the GPS data of a member vehicle and can generate a distributed control signal ensuring the vehicles can maintain the platoon under such attack. The vehicles in the platoon estimate their absolute and relative states (positions and speeds) using GPS data and car sensors, respectively, and then communicate their states using wifi with the neighbors. It is proved that the estimation errors are asymptotically bounded, and using such conditions, the cars can detect if a member vehicle's GPA is under attack.

On the other hand, in [28], the authors introduced vehicle platooning disruption attacks, where an attacker destabilizes or takes control of a platoon through false data injection and replay of control messages. They employ stochastic time series analysis to measure the deviation anomalies of the vehicles from the platoon's expected trajectory and also apply a reputation-based information fusion technique to determine the reliability of received messages. In another study [29], four types of attacks are considered on a platoon of autonomous vehicles, namely 1) spoofing; 2) message falsification; 3) DoS, and 4) burst transmission. An adaptive synchronization-based control algorithm embedding a distributed mitigation mechanism of malicious information was proposed and simulated with the success of platooning operation under such attacks. Attack detection and resilient platooning operation are further investigated in [30], [31] [32].

Attacks on CAN disrupt the communication between ECUs and the ADAS units to initiate false actuation signals. In [180] a neural network-based model is proposed to authenticate electronic messages sent by ECU through CAN to ensure confidentiality and integrity. It exploits the unique transient response parameters of the CAN channel imposed in ECU signals to generate features that can then differentiate individual ECUs. Studies in [181] addresses the cyber-attacks where the attacker infiltrates through vulnerable components of an AV and then masquerades malicious actuation commands and sensing data. CAN frames sent periodically by ADAS be converted into a data stream to extract optimal Time-series bitmap parameters. Euclidean distance between two bitmaps is then compared with a threshold to produce an indication of masqueraded messages.

Safe ITS operations under faulty data injection attacks are discussed in [26]. It uses the optimal threshold levels of sensors to detect DIA attacks when the prior state of the vehicle is known. On the other hand, for a vehicle with no prior information about its state, a multi-armed bandit algorithm is proposed using the Mahalanobis distance between the sensor data and an a-posteriori prediction of the data.

Remote controlling of autonomous vehicles under cyber-attacks are also considered a mitigation technique, and for that, the exact pose (velocity and position) of a vehicle needs to be determined even under the cyber attacks. Studies in [182], [183] present such mechanisms to estimate the vehicles' state. The exact position of a vehicle was determined under GPS spoofing attack and LIDAR replay attack in [183]. Considering the use of an Extended Kalman Filter (EKF) to fuse sensor measurements to estimate a vehicle's own pose, a Cumulative Sum (CUSUM) detector was designed based on the residual of EKF. The specific sensor under attack was identified to reconfigure the EKF so that the secure pose of a vehicle can be estimated under cyber attacks. On the other hand, any attack on communication channels between the AV sensors and the remote controlling station was detected and

mitigated in [182] using an optimal state estimation algorithm based on the mean square error principle.

The security models discussed in this section mainly address the safe operation of ITS under cyber-attacks, and more such models will be seen in upcoming years.

## VIII. FUTURE RESEARCH CHALLENGES

Even though self-driving cars, in conjunction with ITS, have great potentials, and with the gradual acceptance and adoption by people, will perhaps revolutionize transportation and supply chain, in order to build a safe and secure driving environment, there are several open research problems, and issues need to be addressed. The algorithms used in autonomous functions in cars and ITS applications lack reliability in terms of maintaining local laws and the communication methods of different traffic infrastructures in different states or countries. For safe operations of vehicles, there exists a shortage of proper monitoring of different types of road signs depending on the different weather and road conditions. Analysing the current research trend on addressing cybersecurity of AVs and ITS, we have compiled the following research issues that need to be addressed before the use of self-driving cars on a global scale.

- Attacks on Sensors: Sensors perceive the environment the AVs operate in, and any attack on sensors would be detrimental, forcing the car to make wrong decisions with serious consequences. The attackers can target any sensor of an AV and try to fool the vehicle by presenting with tempered data. For example, stop signs with added small graffiti or art stickers could be hard to be recognized by computer vision systems. Inserting fake objects could force the car to stop or slow down unnecessarily, whereas deleting a real object could lead to accidents. Technological advancement makes it easy for the attacker to achieve such tempering with the sensor signals, especially with Lidar sensors, as demonstrated in [25], [178] [179], along with the physical tempering of road signals. New ways can be engineered to launch dangerous attacks like emergency brake or AV freezing attack, where the car can suddenly stop or be remained stop in an intersection even after the red signal turns green. Object detection algorithms must be robust enough to detect in real-time whether an object has been deleted from the vision system or any fake objects are inserted.
- Resilient operation under cyber-attacks: Currently, most of the AVs work in a Test environment, and the research focus is to make the security tighten to avoid cyber-attacks. When AVs take over the road traffic, it will be important to detect whether a vehicle is under attack and continue to operate by isolating the problem areas. Current research trends are shifting towards achieving this goal of safe operation under cyber-attacks [24], [25] [26]. Vehicle platooning is a great example of such research focus, where the platoon vehicles can detect a malicious member and take decisions without any input from the node under attack [27], [28] [29], [30] [31], [32]. It is important to model the attack parameters or signals, i.e., replay attack, spoofing attack and false data injection attack, within the vehicle operation model so that the attack signals can be isolated and filtered out before using it for decision making. As an example, stochastic time series analysis is used to measure the deviation anomalies of the platooning vehicles from the platoon's expected trajectory under false data injection and replay of control messages [28]
- Remote controlling AVs: Another research area that needs more attention is the remote control of an AV under attack. When an autonomous vehicle is under attack, its operations need to be delegated to the drivers, or it can be controlled remotely, which would be more appropriate for freight vehicles. The determination of vehicle pose (position and velocity) is the key to control a vehicle remotely, and deployment of IoT sensors in ITS would be the solution for vehicle pose computation [182], [183]. However, the data communicated to the remote center through wireless channels could potentially be under attack. Any such attack signals need to be modeled so that it can be isolated from any decision making. Once detected, these attack signals could be jammed using a technique where a jammer(s), friendly to the AV and remote center, will only block attackers without hampering legitimate communication [184].
- Adversarial Machine Learning: Autonomous cars utilize machine learning algorithms, especially deep learning models, for decision making at different levels. However, ML techniques are vulnerable to carefully crafted adversarial perturbations. The imperfect training process, the difference in statistical distributions for training and operation data, the learning process being hardly interpretable encourage the adversaries to attack the ML system deployed in AV. Although adversarial attacks on object detection from image have been studied broadly, the same for Lidar point cloud and radar data have been less explored, thus still poses cyber-threat to AV and need research attention [185]. Adversarial data generation and model retraining techniques play a major role in making machine learning techniques robust and trustworthy. Recently, a retraining technique with intelligently selected adversarial samples has been proposed for detecting malware in industrial IoT applications with promising results [186]. Similar techniques can be explored to design learning models highly robust against adversarial attacks in ITS and AVs.
- Attacks on CAN: Controller Area Network (CAN) is a legacy system that has been used as a communication channel between ECUs. A million lines of software code are equipped in an AV. All rely on CAN to function. Being a legacy system, it is continuously being exposed to cyber-threats, which need to be addressed thoroughly,

**TABLE 7. Research challenges for potential attacks and their possible impacts on self-driving cars.**

| Research Challenges | Potential Impact |
|---|---|
| How many sensors are needed to have adequate redundancy? | • Inadequate utilisation of sensors can allow an attacker to build 'blind spots' with possible fatal implications.<br>• Sensor redundancy could be exploited to detect particular sensors under attack and to make correct decisions using an optimal subset of available sensors. |
| What effects can ECUs and CANs be compromised? | • Compromising functionality of the ECU and CAN could drastically change the functionality of vehicles and carry out unsafe activities<br>• Hand over the operation of AV to the driver with proper instructions when ECU/CAN under attack and trigger for remote controlling of the car |
| How is ECU/CAN functionality to be upgraded on a wide scale and safeguarded? | • Without proper security policy and mechanisms, a wide-scale ECU/CAN software update will result in many vulnerabilities in the systems<br>• Alongside mechanical servicing, a practicable car cybersecurity servicing mechanism needs to be devised |
| What are the personal information produced and processed on a vehicle and how can it be used? | • Large amounts of personal data can be produced without the knowledge of passengers<br>• Privacy violations can occur if data is acquired illegally<br>• CAV monetization will accelerate theft of data |
| How does the vehicle detect and operate a cyber threat? | • An AV needs to continuously monitor it's system and detect any cyber-attack as soon as possible<br>• The AV under attack needs to take countermeasure to operate safely under such attack |
| How can it combat the possible increase of its computing power by use of encryption protocols? | • If safety measures are fragile and not purposeful over the expected life expectancy of the vehicle it may render infrastructure and vehicles fragile |
| How to protect users from targeted attacks (phishing, ransomware)? | • The attacker aims to maximise the effectiveness of the attack<br>• Possible financial risk if the consumer pays for any malware cleaning of their vehicle |
| What does a manufacturer response to a big cyber-attack? | • Broad attack surface makes it hard for manufacturer to address the attack, especially when car components are collected from several OEMs.<br>• The supplier could not react to a security breach and the proprietors could be left exposed |
| How can a CAV be used for digital forensics with the additional computing power. | • The lack of evidence of attacks could affect criminal prosecution.<br>• The absence of a public trust will result in the likelihood of modified historical information (i.e., milometers) |
| How do manufacturers follow a information security culture in the production process? | • If businesses do not work under a safety-centered strategy, vulnerabilities will still exist<br>• Security needs to be implemented alongside the driving functionality<br>• Cultural shift required to test million lines of code and automatic real-world traffic scenario based testing needs to be devised |
| How can CAVs detect and avoid unfavourable autonomous DoS attack activity? | • Unusable vehicle functions can be triggered by simplified attack on networks<br>• Important communication protocols for V2V and V2I could impact navigation and collision avoidance systems |
| How to educate users to detect and prevent large-scale automated attacks? | • Automated attacks can be used to quickly classify compromised vehicles<br>• Lack of the requisite expertise would enable non-experts to conduct attacks and can cause serious damage |
| How to reduce exploiting navigation mechanisms? | • Get remote access over the autonomous features of a vehicle<br>• Hijacking of important vehicle equipment |
| How to detect and prevent the attacks on primal low-level sensors? | • Uncertain or unknown may driving instructions may trigger unexpected vehicle activities<br>• More robust algorithms are to be devised to detect such attacks |

otherwise implementing the strongest cybersecurity for all subsystems in a car would not guarantee the car being secured from cyber-attacks. The CAN network needs continuous monitoring for any cyber-attack being detected, and more research needs to be done to make CAN as a secure communication media for AVs' subsystems [181], [187]. Machine learning-based models can be used to monitor CAN to detect any anomalies in signals transmitted through CAN.

- Broader Scope of Cyber-attacks: The attack surface of an AV is relatively very large, considering a car is a final product assembled from many components supplied by the Original Equipment Manufacturer (OEM). The manufacturers need to make sure every such component can combat cyberattacks and also make sure the communication between those components is also secured. Unlike other cyber systems where security comes after the functionality, AV manufacturers need to intertwine cybersecurity with functionality that can only be achievable if they make it an organizational culture to embrace the importance of cybersecurity. This would be one of the main challenges for AV to occupy the road.

New technologies used in self-driving cars and ITS systems in different countries have not been thoroughly tested on roads with real traffic scenarios. As a consequence, the potential attacks and their possible consequences are not clearly understood by the relevant research communities and stakeholders. Table 7 further summarizes the major research challenges discussed above [101], [188]–[191] and their impacts that need to be addressed shortly.

## IX. CONCLUSION

Automobile industries, technology giants, and governments around the world are taking bold initiatives to build safe and affordable autonomous vehicles and market them as early as possible [192], [193]. While this is the biggest technological breakthrough in transportation and driving experience, this can only be realized by making the self-driving vehicles secured and resilient against any kind of cyber-attacks. This paper discusses the security issues surrounding self-driving cars and ITS and defines the strict security requirements that must be adhered to for the widespread acceptance of such vehicles by the community. It lists and analyzes the nature and characteristics of recent notable attacks on self-driving cars as well as potential attacks in the future that might be possible with the current and projected technologies. The possible countermeasures of those attacks are outlined, and their strengths and limitations are discussed. Finally, the paper presents the research gap and future challenges that must be addressed before self-driving cars are permitted to hit the road.

Security attacks change their nature as new applications and technologies are not free from vulnerabilities, and the new ones are discovered on a regular basis. Countermeasure techniques based on cryptography, access control, authentication mechanism, and physical layer hardware and communication security also continue to evolve. In this dynamic and exciting research scope, this paper presents a very good foundation knowledge to the researchers from academia and industry.

## REFERENCES

[1] X. Hu, Y.-C. Chiu, J. A. Villalobos, and E. Nava, "A sequential decomposition framework and method for calibrating dynamic origin—Destination demand in a congested network," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 10, pp. 2790–2797, Feb. 2017.

[2] A. Y. and M. A., "Adaptive case management framework to develop case-based emergency response system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 4, pp. 57–66, 2017.

[3] J. K. Kim, R. Sharman, H. R. Rao, and S. Upadhyaya, "Efficiency of critical incident management systems: Instrument development and validation," *Decis. Support Syst.*, vol. 44, no. 1, pp. 235–250, Nov. 2007.

[4] S. Akhtar Ali Shah, H. Kim, S. Baek, H. Chang, and B. H. Ahn, "System architecture of a decision support system for freeway incident management in republic of korea," *Transp. Res. A, Policy Pract.*, vol. 42, no. 5, pp. 799–810, Jun. 2008.

[5] Y. Wang, G. Tan, Y. Wang, and Y. Yin, "Perceptual control architecture for cyber–physical systems in traffic incident management," *J. Syst. Archit.*, vol. 58, no. 10, pp. 398–411, Nov. 2012.

[6] J. H. Lambert, A. I. Parlak, Q. Zhou, J. S. Miller, M. D. Fontaine, T. M. Guterbock, J. L. Clements, and S. A. Thekdi, "Understanding and managing disaster evacuation on a transportation network," *Accident Anal. Prevention*, vol. 50, pp. 645–658, Jan. 2013.

[7] Y. A. Rebeeh, S. Pokharel, G. M. Abdella, and A. S. Hammuda, "Disaster management in industrial areas: Perspectives, challenges and future research," *J. Ind. Eng. Manage.*, vol. 12, no. 1, pp. 133–153, 2019.

[8] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 22–28, Mar. 2017.

[9] J.-A. Jang, K. Choi, and H. Cho, "A fixed sensor-based intersection collision warning system in vulnerable line-of-sight and/or traffic-violation-prone environment," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 4, pp. 1880–1890, Dec. 2012.

[10] A. Nikitas, E. T. Njoya, and S. Dani, "Examining the myths of connected and autonomous vehicles: Analysing the pathway to a driverless mobility paradigm," *Int. J. Automot. Technol. Manage.*, vol. 19, nos. 1–2, pp. 10–30, 2019.

[11] J. Evans, "Governing cities for sustainability: A research agenda and invitation," *Frontiers Sustain. Cities*, vol. 1, p. 2, Jun. 2019.

[12] Y. Choi and S.-W. Rhee, "Current status and perspectives on recycling of end-of-life battery of electric vehicle in korea (Republic of)," *Waste Manage.*, vol. 106, pp. 261–270, Apr. 2020.

[13] B. L. Bollinger, "The security and privacy in your car act: Will it actually protect you," *North Carolina J. Law Technol.*, vol. 18, no. 5, p. 214, 2017.

[14] H. Lim and A. Taeihagh, "Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications," *Energies*, vol. 11, no. 5, p. 1062, Apr. 2018.

[15] N. Thompson, A. Mullins, and T. Chongsutakawewong, "Does high e-government adoption assure stronger security? Results from a cross-country analysis of australia and thailand," *Government Inf. Quart.*, vol. 37, no. 1, Jan. 2020, Art. no. 101408.

[16] N. Tan, "Electoral management of digital campaigns and disinformation in east and southeast asia," *Election Law J., Rules, Politics, Policy*, vol. 19, no. 2, pp. 214–239, Jun. 2020.

[17] S. Feng, Y. Feng, X. Yan, S. Shen, S. Xu, and H. X. Liu, "Safety assessment of highly automated driving systems in test tracks: A new framework," *Accident Anal. Prevention*, vol. 144, Sep. 2020, Art. no. 105664.

[18] M. C. Coelho and C. Guarnaccia, "Driving information in a transition to a connected and autonomous vehicle environment: Impacts on pollutants, noise and safety," *Transp. Res. Procedia*, vol. 45, pp. 740–746, Jan. 2020.

[19] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.

[20] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101823.

[21] B. Schoettle and M. Sivak, "A survey of public opinion about autonomous and self-driving vehicles in the US, the UK, and Australia," Transp. Res. Inst., Univ. Michigan, Ann Arbor, MI, USA, Tech. Rep. UMTRI-2014-21, 2014.
[22] M. Teichmann, M. Weber, M. Zollner, R. Cipolla, and R. Urtasun, "MultiNet: Real-time joint semantic reasoning for autonomous driving," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2018, pp. 1013–1020.
[23] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, "Enhancements of V2X communication in support of cooperative autonomous driving," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 64–70, Dec. 2015.
[24] M. Porter, S. Dey, A. Joshi, P. Hespanhol, A. Aswani, M. Johnson-Roberson, and R. Vasudevan, "Detecting deception attacks on autonomous vehicles via linear time-varying dynamic watermarking," 2020, *arXiv:2001.09859*. [Online]. Available: http://arxiv.org/abs/2001.09859
[25] R. Changalvala and H. Malik, "LiDAR data integrity verification for autonomous vehicle," *IEEE Access*, vol. 7, pp. 138018–138031, 2019.
[26] A. Ferdowsi, S. Ali, W. Saad, and N. B. Mandayam, "Cyber-physical security and safety of autonomous connected vehicles: Optimal control meets multi-armed bandit learning," *IEEE Trans. Commun.*, vol. 67, no. 10, pp. 7228–7244, Oct. 2019.
[27] X. He, E. Hashemi, and K. H. Johansson, "Secure platooning of autonomous vehicles under attacked GPS data," 2020, *arXiv:2003.12975*. [Online]. Available: http://arxiv.org/abs/2003.12975
[28] N. Bermad, S. Zemmoudj, and M. Omar, "Securing vehicular platooning against vehicle platooning disruption (VPD) attacks," in *Proc. 8th Int. Conf. Perform. Eval. Modeling Wired Wireless Netw. (PEMWN)*, Nov. 2019, pp. 1–6.
[29] A. Petrillo, A. Pescape, and S. Santini, "A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks," *IEEE Trans. Cybern.*, early access, Jan. 23, 2020, doi: 10.1109/TCYB.2019.2962601.
[30] T. Keijzer and R. M. G. Ferrari, "A sliding mode observer approach for attack detection and estimation in autonomous vehicle platoons using event triggered communication," in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, Dec. 2019, pp. 5742–5747.
[31] W. Jeon, Z. Xie, A. Zemouche, and R. Rajamani, "Simultaneous cyber-attack detection and radar sensor health monitoring in connected ACC vehicles," *IEEE Sensors J.*, early access, Jul. 24, 2020, doi: 10.1109/JSEN.2020.3011698.
[32] Z. Li, Z. Li, and Y. Liu, "Resilient control design of the third-order discrete-time connected vehicle systems against cyber-attacks," *IEEE Access*, vol. 8, pp. 157470–157481, 2020.
[33] B. L. Bollinger, "The security and privacy in your car act: Will it actually protect you," *North Carolina J. Law Technol.*, vol. 18, no. 5, p. 214, 2017.
[34] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.
[35] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, May 2017.
[36] M. Buinevich and A. Vladyko, "Forecasting issues of wireless communication Networks' cyber resilience for an intelligent transportation system: An overview of cyber attacks," *Information*, vol. 10, no. 1, p. 27, Jan. 2019.
[37] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, "Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review," *Comput. Electr. Eng.*, vol. 86, Sep. 2020, Art. no. 106717.
[38] F. Sommer, J. Dürrwang, and R. Kriesten, "Survey and classification of automotive security attacks," *Information*, vol. 10, no. 4, p. 148, Apr. 2019.
[39] A. Bazzi, B. M. Masini, A. Zanella, and I. Thibault, "On the performance of IEEE 802.11p and LTE-V2 V for the cooperative awareness of connected vehicles," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10419–10432, Nov. 2017.
[40] W. Sun, J. Liu, and H. Zhang, "When smart wearables meet intelligent vehicles: Challenges and future directions," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 58–65, Jun. 2017.
[41] A. M. Dahod, A. Schoener, K. Chowdhury, L. Schwartz, M. H. Harper, K. E. Virgile, and A. Gibbs, "Adaptive intelligent routing in a communication system," U.S. Patent 9 565 117, Feb. 7, 2017.
[42] Y. Tang, C. Zhang, R. Gu, P. Li, and B. Yang, "Vehicle detection and recognition for intelligent traffic surveillance system," *Multimedia Tools Appl.*, vol. 76, no. 4, pp. 5817–5832, Feb. 2017.
[43] R. Kolandaisamy, R. M. Noor, I. Ahmedy, I. Ahmad, M. R. Z'aba, M. Imran, and M. Alnuem, "A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–13, May 2018.
[44] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks–practical examples and selected short-term countermeasures," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Berlin, Germany: Springer, 2008, pp. 235–248.
[45] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Secur. Symp. (USENIX Secur.)*, vol. 4, 2011, pp. 447–462.
[46] J. Golson, "Car hackers demonstrate wireless attack on tesla model s," *Verge*, vol. 19, 2016.
[47] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *Int. J. Netw. Secur. Appl.*, vol. 5, no. 5, p. 95, 2013.
[48] T. Adachi, R. Hiura, T. Fukase, and T. Okazaki, "On-board unit and fault determination method," U.S. Patent 10 126 922, Nov. 13, 2018.
[49] S. Elitzur, V. Rosenband, and A. Gany, "On-board hydrogen production for auxiliary power in passenger aircraft," *Int. J. Hydrogen Energy*, vol. 42, no. 19, pp. 14003–14009, May 2017.
[50] S. H. Bouk, S. H. Ahmed, D. Kim, and H. Song, "Named-data-networking-based ITS for smart cities," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 105–111, Jan. 2017.
[51] S. Mirri, C. Prandi, P. Salomoni, F. Callegati, A. Melis, and M. Prandini, "A service-oriented approach to crowdsensing for accessible smart mobility scenarios," *Mobile Inf. Syst.*, vol. 2016, pp. 1–14, Jan. 2016.
[52] H. Vahdat-Nejad, A. Ramazani, T. Mohammadi, and W. Mansoor, "A survey on context-aware vehicular network applications," *Veh. Commun.*, vol. 3, pp. 43–57, Jan. 2016.
[53] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it—On the (in) security of automotive remote keyless entry systems," in *Proc. 25th USENIX Secur. Symp. (USENIX Secur.)*, 2016, pp. 1–16.
[54] D. D. Miller, "Systems and methods to detect vehicle queue lengths of vehicles stopped at a traffic light signal," U.S. Patent 15 091 170, Jul. 20, 2017.
[55] R. I. Meneguette, R. De Grande, and A. A. Loureiro, *Intelligent Transport System in Smart Cities*. Cham, Switzerland: Springer, 2018.
[56] K. Ansari, "Cloud computing on cooperative cars (C4S): An architecture to support Navigation-as-a-Service," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, Jul. 2018, pp. 794–801.
[57] R. Zhang, F. Schmutz, K. Gerard, A. Pomini, L. Basseto, S. B. Hassen, A. Jaiprakash, I. Ozgunes, A. Alarifi, H. Aldossary, I. AIKurtass, O. Talabay, A. AlMhanna, S. AlGhamisi, M. AlSaleh, A. A. Biyabani, K. Al-Ghoneim, and O. K. Tonguz, "Increasing traffic flows with DSRC technology: Field trials and performance evaluation," in *Proc. IECON 44th Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2018, pp. 6191–6196.
[58] K. Zheng, L. Hou, H. Meng, Q. Zheng, N. Lu, and L. Lei, "Soft-defined heterogeneous vehicular network: Architecture and challenges," *IEEE Netw.*, vol. 30, no. 4, pp. 72–80, Jul. 2016.
[59] T. Kryjak, M. Komorkiewicz, and M. Gorgon, "Real-time hardware–software embedded vision system for ITS smart camera implemented in zynq SoC," *J. Real-Time Image Process.*, vol. 15, no. 1, pp. 123–159, Jun. 2018.
[60] V. Dhilip Kumar, P. Chyne, D. Kandar, and B. S. Paul, "Performance analysis of hybrid WiMAX/DSRC scenarios for vehicular communication environment," *Microsyst. Technol.*, vol. 23, no. 9, pp. 4231–4236, Sep. 2017.
[61] B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: A survey," *J. Netw. Comput. Appl.*, vol. 40, pp. 363–396, Apr. 2014.
[62] F. Cunha, A. Boukerche, L. Villas, A. Viana, and A. A. F. Loureiro, "Data communication in VANETs: A survey, challenges and applications," *Netw., IEEE Commun. Surveys Tuts.*, 2014.
[63] M. Javed, E. Ben Hamida, and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice," *Sensors*, vol. 16, no. 6, p. 879, Jun. 2016.
[64] M. A. Javed and E. B. Hamida, "On the interrelation of security, QoS, and safety in cooperative ITS," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 7, pp. 1943–1957, Jul. 2017.

[65] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Veh. Commun.*, vol. 12, pp. 138–164, Apr. 2018.

[66] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "A review of threat analysis and risk assessment methods in the automotive context," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Cham, Switzerland: Springer, 2016, pp. 130–141.

[67] S. Gisdakis, M. Lagana, T. Giannetsos, and P. Papadimitratos, "SEROSA: SERvice oriented security architecture for vehicular communications," in *Proc. IEEE Veh. Netw. Conf.*, Dec. 2013, pp. 111–118.

[68] F. Han, L. Lin, and S. Li, "Invulnerability analysis in intelligent transportation system," *Int. J. High Perform. Syst. Archit.*, vol. 7, no. 4, pp. 197–203, 2017.

[69] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the Internet of vehicles," *Ann. Telecommun.*, vol. 72, nos. 5–6, pp. 283–295, 2017.

[70] I. Balabine and A. Velednitsky, "Method and system for confident anomaly detection in computer network traffic," U.S. Patent 9 843 488, Dec. 12, 2017.

[71] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and T. Saha, "Detecting intrusion in the traffic signals of an intelligent traffic system," in *Proc. Int. Conf. Inf. Commun. Secur.* Cham, Switzerland: Springer, 2018, pp. 696–707.

[72] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 817–824, Jan. 2018.

[73] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, Mar. 2019.

[74] J. E. Siegel, D. C. Erb, and S. E. Sarma, "A survey of the connected vehicle landscape—Architectures, enabling technologies, applications, and development areas," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2391–2406, Oct. 2017.

[75] A. O. A. Zaabi, C. Y. Yeun, and E. Damiani, "Autonomous vehicle security: Conceptual model," in *Proc. IEEE Transp. Electrific. Conf. Expo, Asia–Pacific (ITEC Asia–Pacific)*, May 2019, pp. 1–5.

[76] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017.

[77] E. R. Teoh and D. G. Kidd, "Rage against the machine? Google's self-driving cars versus human drivers," *J. Saf. Res.*, vol. 63, pp. 57–60, Dec. 2017.

[78] W. Qi, Q. Song, X. Wang, L. Guo, and Z. Ning, "SDN-enabled social-aware clustering in 5G-VANET systems," *IEEE Access*, vol. 6, pp. 28213–28224, 2018.

[79] M. Baza, M. Nabil, M. M. E. A. Mahmoud, N. Bewermeier, K. Fidan, W. Alasmary, and M. Abdallah, "Detecting sybil attacks using proofs of work and location in VANETs," *IEEE Trans. Depend. Sec. Comput.*, early access, May 11, 2020, doi: 10.1109/TDSC.2020.2993769.

[80] S. Alam, S. Sulistyo, I. W. Mustika, and R. Adrian, "Review of potential methods for handover decision in V2 V VANET," in *Proc. Int. Conf. Comput. Sci., Inf. Technol., Electr. Eng. (ICOMITEE)*, Oct. 2019, pp. 237–243.

[81] C. Schmittner, S. Chlup, A. Fellner, G. Macher, and E. Brenner, "ThreatGet: Threat modeling based approach for automated and connected vehicle systems," in *Proc. AmE Automot. Meets Electron., 11th GMM-Symp.*, 2020, pp. 1–3.

[82] M. Dibaei, X. Zheng, K. Jiang, S. Maric, R. Abbas, S. Liu, Y. Zhang, Y. Deng, S. Wen, J. Zhang, Y. Xiang, and S. Yu, "An overview of attacks and defences on intelligent connected vehicles," 2019, *arXiv:1907.07455*. [Online]. Available: http://arxiv.org/abs/1907.07455

[83] C. Schartmüller, K. Weigl, P. Wintersberger, A. Riener, and M. Steinhauser, "Text comprehension: heads-up vs. Auditory displays: Implications for a productive work environment in SAE level 3 automated vehicles," in *Proc. 11th Int. Conf. Automot. User Interface Interact. Veh. Appl.*, Sep. 2019, pp. 342–354.

[84] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang, and X. Zhou, "Multi-channel based sybil attack detection in vehicular ad hoc networks using RSSI," *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 362–375, Feb. 2019.

[85] C. Xu, M. Ma, X. Huang, and H. Bao, "A cross-domain group authentication scheme for LTE–A based vehicular network," in *Proc. IEEE 9th Int. Conf. Commun. Softw. Netw. (ICCSN)*, May 2017, pp. 595–599.

[86] J. Lin, W. Yu, N. Zhang, X. Yang, and L. Ge, "Data integrity attacks against dynamic route guidance in transportation-based cyber-physical systems: Modeling, analysis, and defense," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8738–8753, Sep. 2018.

[87] S. S. Albouq and E. M. Fredericks, "Lightweight detection and isolation of black hole attacks in connected vehicles," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Jun. 2017, pp. 97–104.

[88] M. Pawar and J. Agarwal, "A literature survey on security issues of wsn and different types of attacks in network," *Indian J. Comput. Sci. Eng*, vol. 8, pp. 80–83, 2017.

[89] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 10–21, Feb. 2014.

[90] A. Greenberg. (2016). *The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse. Wired, August 1, 2016*. Accessed: Aug. 15, 2017. [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-a%cceleration-hacks/

[91] M. Schellekens, "Car hacking: Navigating the regulatory landscape," *Comput. Law Secur. Rev.*, vol. 32, no. 2, pp. 307–315, Apr. 2016.

[92] S. Zhang, J. Chen, F. Lyu, N. Cheng, W. Shi, and X. Shen, "Vehicular communication networks in the automated driving era," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 26–32, Sep. 2018.

[93] 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.

[94] M. Wolf, R. Lambert, T. Enderle, and A. Schmidt, "Wanna drive? Feasible attack Paths and effective protection against ransomware in modern vehicles," in *Proc. Embedded Secur. Cars Conf. (escar) Eur.*, 2017, pp. 1–14.

[95] L. M. Cysneiros, M. Raffi, and J. C. Sampaio do Prado Leite, "Software transparency as a key requirement for self-driving cars," in *Proc. IEEE 26th Int. Requirements Eng. Conf. (RE)*, Aug. 2018, pp. 382–387.

[96] I. Yaqoob, L. U. Khan, S. M. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 174–181, Jan. 2020.

[97] A. Hakkala and O. I. Heimo, "Automobile automation and lifecycle: How digitalisation and security issues affect the car as a product and service," in *Proc. SAI Intell. Syst. Conf.*, Springer, 2019, pp. 121–137.

[98] 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.

[99] M. Pham and K. Xiong, "A survey on security attacks and defense techniques for connected and autonomous vehicles," 2020, *arXiv:2007.08041*. [Online]. Available: http://arxiv.org/abs/2007.08041

[100] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Eur.*, vol. 11, 2015, p. 2015.

[101] A. Taeihagh and H. S. M. Lim, "Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks," *Transp. Rev.*, vol. 39, no. 1, pp. 103–128, Jan. 2019.

[102] Y. Zhao, "Telematics: Safe and fun driving," *IEEE Intell. Syst.*, vol. 17, no. 1, pp. 10–14, Jan. 2002.

[103] M. Wolf and C. Paar, "Security requirements engineering in the automotive domain: On specification procedures and implementational aspects," in *Proc. SICHERHEIT Sicherheit, Schutz Und Zuverlaíassigkeit. Beitraíage der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft Fuíar Informatik eV (GI)*, 2008, pp. 485–498.

[104] T. Zaidi and S. Faisal, "An overview: Various attacks in VANET," in *Proc. 4th Int. Conf. Comput. Commun. Autom. (ICCCA)*, Dec. 2018, pp. 1–6.

[105] M. Dikmen and C. M. Burns, "Autonomous driving in the real world: Experiences with tesla autopilot and summon," in *Proc. 8th Int. Conf. Automot. User Interface Interact. Veh. Appl. - Automotive'UI*, 2016, pp. 225–228.

[106] A. M. Nascimento, L. F. Vismari, P. S. Cugnasca, J. Camargo, J. de Almeida, R. Inam, E. Fersman, A. Hata, and M. Marquezini, "Concerns on the differences between ai and system safety mindsets impacting autonomous vehicles safety," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Cham, Switzerland: Springer, 2018, pp. 481–486.

[107] A. Herm, (2017). *Assume Self-Driving Cars are a Hacker's Dream? Think Again*. Guardian. Accessed: 2018. [Online]. Available: https://www.theguardian.com/technology/2017/aug/30/self-driving-cars-hackers-security.Zugegriffenam
[108] M. Cheah, S. A. Shaikh, O. Haas, and A. Ruddle, "Towards a systematic security evaluation of the automotive Bluetooth interface," *Veh. Commun.*, vol. 9, pp. 8–18, Jul. 2017.
[109] S. Prevost and H. Kettani, "On data privacy in modern personal vehicles," in *Proc. 4th Int. Conf. Big Data Internet Things*, Oct. 2019, pp. 1–4.
[110] J. Stewart, "Tesla's autopilot was involved in another deadly car crash," *Wired*, vol. 3, p. 30, Mar. 2018.
[111] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 546–556, Apr. 2015.
[112] S. Garfinkel. (2017). *Hackers Are the Real Obstacle for Self-Driving Vehicles*. MIT Technology Review. Accessed: Oct. 16, 2020. [Online]. Available: https://www.technologyreview.com/s/608618/hackers-are-the-real-obstacle-for-self-driving-vehicles/
[113] F. Sun, T. Jones, and S. Lennox, "Enhancing autonomous vehicle perception with off-vehicle collected data," U.S. Patent 10 101 745, Oct. 16, 2018.
[114] S. Bruneel, "The fast and furiously approaching need for legal regulation of autonomous driving," *Brigham Young Univ. Prelaw Rev.*, vol. 30, no. 1, p. 7, 2016.
[115] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.
[116] L. ben Othmane, L. Dhulipala, M. Abdelkhalek, M. Govindarasu, and N. Multari, "Detection of injection attacks in in-vehicle networks," in *Proc. Electr. Comput. Eng. Conf. Papers, Posters Presentations*, 2019.
[117] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, Aug. 2015.
[118] D. Lodge, "Hacking the mitsubishi outlander PHEV hybrid," *PenTestPartners*, vol. 5, Jun. 2016. Accessed: Oct. 16, 2020. [Online]. Available: https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/
[119] K. Stępiń and A. Poniszewska-Marańda, "Security solution methods in the vehicular ad-hoc networks," in *Proc. 17th Int. Conf. Adv. Mobile Comput. Multimedia*, Dec. 2019, pp. 127–135.
[120] M. Hirz and B. Walzel, "Sensor and object recognition technologies for self-driving cars," *Comput.-Aided Des. Appl.*, vol. 15, no. 4, pp. 501–508, Jul. 2018.
[121] J. Fayyad, M. A. Jaradat, D. Gruyer, and H. Najjaran, "Deep learning sensor fusion for autonomous vehicle perception and localization: A review," *Sensors*, vol. 20, no. 15, p. 4220, Jul. 2020.
[122] R. Islam and R. U. D. Refat, "Improving CAN bus security by assigning dynamic arbitration IDs," *J. Transp. Secur.*, vol. 13, nos. 1–2, pp. 19–31, Jun. 2020.
[123] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM 27th Conf. Comput. Commun.*, Apr. 2008, pp. 246–250.
[124] S. P. Sandford and D. F. Pierrottet, "Navigation system for GPS denied environments," U.S. Patent 15 932 639, Oct. 3, 2019.
[125] T. Toyama, H. Oguma, T. Matsumoto, H. Gotoh, and T. Moriya, "System and method for detecting attack when sensor and traffic information are inconsistent," U.S. Patent 16 507 157, Oct. 31, 2019.
[126] S. Mookherji and S. Sankaranarayanan, "Traffic data classification for security in iot-based road signaling system," in *Soft Comput. Data Analytics*. Singapore: Springer, 2019, pp. 589–599.
[127] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc Sensor Wireless Netw.*, vol. 24, nos. 3–4, pp. 283–305, 2015.
[128] M. Jagielski, N. Jones, C.-W. Lin, C. Nita-Rotaru, and S. Shiraishi, "Threat detection for collaborative adaptive cruise control in connected cars," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2018, pp. 184–189.
[129] B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci., Univ. Twente, Enschede, The Netherlands, 2015.
[130] P. Nayak, R. S. U. Suseela, and V. Trivedi, "A review on DoS attack for WSN: Defense and detection mechanisms," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 453–461.
[131] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.
[132] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, p. 1433, May 2018.
[133] J. T. Curran and A. Broumendan, "On the use of low-cost IMUs for GNSS spoofing detection in vehicular applications," in *Proc. ITSNT*, 2017, pp. 1–8.
[134] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Comments on 'dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,'" *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2149–2151, Nov. 2017.
[135] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[136] T. Humphreys, *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*. Austin, TX, USA: Univ. Texas at Austin, Jul. 2012, pp. 1–16.
[137] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protection*, vol. 5, nos. 3–4, pp. 146–153, Dec. 2012.
[138] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time GPS spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267–278, Dec. 2013.
[139] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. Radionavigation Lab. Conf.*, 2008, pp. 1–12.
[140] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: a study of misbehavior in vehicular platoons," in *Proc. 8th ACM Conf. Secur. Privacy Wireless Mobile Netw. - WiSec*, 2015, p. 22.
[141] J. Liu, D. Ma, A. Weimerskirch, and H. Zhu, "A functional co-design towards safe and secure vehicle platooning," in *Proc. 3rd ACM Workshop Cyber-Phys. Syst. Secur. - CPSS*, 2017, pp. 81–90.
[142] K. Wang, L. Wang, and M. Cui, "Trajectory tracking and recovery attacks in VANET systems," *Int. J. Commun. Syst.*, vol. 31, no. 17, Nov. 2018, Art. no. e3797.
[143] T. Ort, L. Paull, and D. Rus, "Autonomous vehicle navigation in rural environments without detailed prior maps," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, May 2018, pp. 2040–2047.
[144] H. T. Cheng, H. Shan, and W. Zhuang, "Infotainment and road safety service support in vehicular networking: From a communication perspective," *Mech. Syst. Signal Process.*, vol. 25, no. 6, pp. 2020–2038, Aug. 2011.
[145] I. Blayvas, R. Fridental, and S. Da, "Systems and methods for autonomous vehicle navigation," U.S. Patent 10 002 471, Jun. 19, 2018.
[146] F. D. Garcia, G. de Koning Gans, R. Verdult, and M. Meriac, "Dismantling iclass and iclass elite," in *Proc. Eur. Symp. Res. Comput. Secur.* Berlin, Germany: Springer, 2012, pp. 697–715.
[147] P. Soni and A. Sharma, "Sybil node detection and prevention approach on physical location in VANET," *Int. J. Comput. Appl.*, vol. 128, no. 16, pp. 38–42, Oct. 2015.
[148] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in VANETs," in *Proc. 4th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2013, pp. 1–6.
[149] M. Bharat, K. S. Sree, and T. M. Kumar, "Authentication solution for security attacks in VANETs," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 8, pp. 7661–7664, 2014.
[150] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K.-R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9390–9401, Sep. 2020.
[151] A. Faisal, T. Yigitcanlar, M. Kamruzzaman, and A. Paz, "Mapping two decades of autonomous vehicle research: A systematic scientometric analysis," *J. Urban Technol.*, vol. 27, pp. 1–30, Aug. 2020.
[152] J. M. Sullivan, M. J. Flannagan, A. K. Pradhan, and S. Bao, "Literature review of behavioral adaptations to advanced driver assistance systems," in *Proc. TRIS ITRD Database*, 2016, pp. 1–55.
[153] K. Suzuki, T. Asao, J.-I. Hayashi, and Y. Miichi, "Safety evaluation of advanced driver assistance systems as human-machine systems," *Int. J. Automot. Eng.*, vol. 8, no. 4, pp. 163–170, 2017.

[154] S. K. Erskine and K. M. Elleithy, "Real-time detection of DoS attacks in IEEE 802.11p using fog computing for a secure intelligent vehicular network," *Electronics*, vol. 8, no. 7, p. 776, Jul. 2019.
[155] M. Islam, M. Chowdhury, H. Li, and H. Hu, "Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2672, no. 19, pp. 66–78, Dec. 2018.
[156] D. Elliott, W. Keen, and L. Miao, "Recent advances in connected and automated vehicles," *J. Traffic Transp. Eng. (English Ed.)*, vol. 6, no. 2, pp. 109–131, Apr. 2019.
[157] V. Linkov, P. Zámečník, D. Havlíčková, and C.-W. Pai, "Human factors in the cybersecurity of autonomous vehicles: Trends in current research," *Frontiers Psychol.*, vol. 10, p. 995, May 2019.
[158] R. Hussain and S. Zeadally, "Autonomous cars: Research results, issues, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1275–1313, 2nd Quart., 2019.
[159] M. Guri and D. Bykhovsky, "AIR-jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR)," *Comput. Secur.*, vol. 82, pp. 15–29, May 2019.
[160] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transp. Res. A, Policy Pract.*, vol. 124, pp. 523–536, Jun. 2019.
[161] A. Costin, "Security of CCTV and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations," in *Proc. 6th Int. Workshop Trustworthy Embedded Devices - TrustED*, 2016, pp. 45–54.
[162] B. Cusack and Z. Tian, "Evaluating ip surveillance camera vulnerabilities," in *Proc. 15th Austral. Inf. Secur. Manage. Conf.*, 2017, pp. 1–9.
[163] J. Raiyn, "Data and cyber security in autonomous vehicle networks," *Transp. Telecommun. J.*, vol. 19, no. 4, pp. 325–334, Dec. 2018.
[164] A.-S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Boca Raton, FL, USA: CRC Press, 2016.
[165] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 524–540, Feb. 2015.
[166] K. Babber and R. Randhawa, "Cross-layer designs in wireless sensor networks," in *Computational Intelligence in Sensor Networks*. Berlin, Germany: Springer, 2019, pp. 141–166.
[167] A. Chowdhury, "Recent cyber security attacks and their mitigation approaches–an overview," in *Proc. Int. Conf. Appl. Techn. Inf. Secur.* Singapore: Springer, 2016, pp. 54–65.
[168] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A sybil attack detection scheme for a forest wildfire monitoring application," *Future Gener. Comput. Syst.*, vol. 80, pp. 613–626, Mar. 2018.
[169] S. Chaba, R. Kumar, R. Pant, and M. Dave, "Secure and efficient key delivery in VANET using cloud and fog computing," in *Proc. Int. Conf. Comput., Commun. Electron. (Comptelix)*, Jul. 2017, pp. 27–31.
[170] A. Muhamad and M. Elhadef, "Sybil attacks in intelligent vehicular ad hoc networks: A review," in *Advanced Multimedia and Ubiquitous Engineering*. Singapore: Springer, 2018, pp. 547–555.
[171] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, "Malicious node identification routing and protection mechanism for vehicular ad-hoc network against various attacks," *Int. J. Netw. Virtual Organisations*, vol. 19, nos. 2–4, pp. 153–175, 2018.
[172] P. Agarwal, "Technical review on different applications, challenges and security in vaNet," *J. Multimedia Technol. Recent Adv*, vol. 4, no. 3, pp. 21–30, 2017.
[173] Deeksha, A. Kumar, and M. Bansal, "A review on VANET security attacks and their countermeasure," in *Proc. 4th Int. Conf. Signal Process., Comput. Control (ISPCC)*, Sep. 2017, pp. 580–585.
[174] M. Jain and R. Saxena, "VaNet: Security attacks, solution and simulation," in *Proc. 2nd Int. Conf. Comput. Intell. Inform.* Singapore: Springer, 2018, pp. 457–466.
[175] E. S. Stolyarova, D. M. Shiryaev, A. G. Vladyko, and M. V. Buinevich, "VANET/ITS cybersecurity threats: Analysis, categorization and forecasting," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Jan. 2018, pp. 136–141.
[176] M. A. H. Al Junaid, A. Syed, M. N. M. Warip, K. N. F. K. Azir, and N. H. Romli, "Classification of security attacks in vanet: A review of requirements and perspectives," in *Proc. MATEC Web Conf.*, vol. 150. Les Ulis, France: EDP Sciences, 2018, Art. no. 06038.
[177] W.-H. Ko, B. Satchidanandan, and P. R. Kumar, "Dynamic watermarking-based defense of transportation cyber-physical systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 1, pp. 1–21, Jan. 2020.
[178] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on LiDAR-based perception in autonomous driving," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 2267–2281.
[179] B. Nassi, D. Nassi, R. Ben-Netanel, Y. Mirsky, O. Drokin, and Y. Elovici, "Phantom of the ADAS: Phantom attacks on driver-assistance systems," *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 85, Oct. 2020.
[180] A. Hafeez, K. Topolovec, and S. Awad, "ECU fingerprinting through parametric signal modeling and artificial neural networks for in-vehicle security against spoofing attacks," in *Proc. 15th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2019, pp. 29–38.
[181] C. Gutierrez, M. Juliato, S. Ahmed, and M. Sastry, "Detecting attacks against safety-critical ADAS based on in-vehicle network message patterns," in *Proc. 49th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. Ind. Track*, Jun. 2019, pp. 9–12.
[182] M. M. Rana, "IoT-based electric vehicle state estimation and control algorithms under cyber attacks," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 874–881, Feb. 2020.
[183] Q. Liu, Y. Mo, X. Mo, C. Lv, E. Mihankhah, and D. Wang, "Secure pose estimation for autonomous vehicles under cyber attacks," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2019, pp. 1583–1588.
[184] J. E. Giti, A. Sakzad, B. Srinivasan, J. Kamruzzaman, and R. Gaire, "Secrecy capacity against adaptive eavesdroppers in a random wireless network using friendly jammers and protected zone," *J. Netw. Comput. Appl.*, vol. 165, Sep. 2020, Art. no. 102698.
[185] 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.
[186] M. E. Khoda, T. Imam, J. Kamruzzaman, I. Gondal, and A. Rahman, "Robust malware defense in industrial IoT applications using machine learning with selective adversarial samples," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4415–4424, Aug. 2019.
[187] H. K. Kalutarage, M. O. Al-Kadri, M. Cheah, and G. Madzudzo, "Context-aware anomaly detector for monitoring cyber attacks on automotive CAN bus," in *Proc. ACM Comput. Sci. Cars Symp. CSCS*, 2019, pp. 1–8.
[188] W. B. Rouse, "The systems, man, and cybernetics of driverless cars: Challenges and opportunities for the SMCS," *IEEE Syst., Man, Cybern. Mag.*, vol. 3, no. 3, pp. 6–8, Jul. 2017.
[189] A. Wolfe, "Unstoppable the gap between public safety and traffic safety in the age of driverless cars," Naval Postgraduate School Monterey, Washington, DC, USA, Reduction Project 0704-0188, 2017.
[190] S. Dadras and C. Winstead, *Cybersecurity of Autonomous Vehicle Platooning*. Logan, Utah: Utah State Univ., 2017.
[191] 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.
[192] I. Autonomous Vehicle Computing Consortium. (2019). *Tackling the Complexities and Obstacles Necessary for Realizing the Development and Volume Production of Safe and Affordable Autonomous Vehicles*. Accessed: Aug. 6, 2020. [Online]. Available: https://www.avcconsortium.org
[193] D. Etherington. (2019). *Toyota, Gm, Nvidia, Bosch and Others Form New Autonomous Driving Tech Consortium*. Accessed: Aug. 6, 2020. [Online]. Available: https://tcrn.ch/3mndbJT

**ABDULLAHI CHOWDHURY** (Member, IEEE) received the bachelor of information technology degree from Central Queensland University, Australia, in 2004, the master of information technology degree from Monash University, Australia, in 2006, and the Ph.D. degree from Federation University Australia, in 2020. He worked as a Lecturer with the Royal University of Dhaka, Bangladesh, from 2006 to 2007, and has been working in various positions in Telstra, Australian Taxation Office, and Australia Post, since 2008. His research interests include intelligent transportation systems, the IoT, and machine learning.

**GOUR KARMAKAR** (Member, IEEE) received the B.Sc. degree in CSE from BUET, in 1993, and the master's and Ph.D. degrees in information technology from the Faculty of Information Technology, Monash University, in 1999 and 2003, respectively. He is currently a Senior Lecturer with Federation University Australia. He has published over 156 peer-reviewed research publications, including 36 international peer-reviewed reputed journal articles and was awarded six best papers in reputed international conferences. He received a prestigious ARC linkage grant in 2011. He has successfully supervised 14 Ph.D. and four Masters by research projects from the commencement to completion. One of his Ph.D. students received both Mollie Holman Doctoral and Faculty of Information Technology Doctoral Medals in 2009. His research interests include multimedia signal processing, big data analytics, the Internet of Things, and cybersecurity, including trustworthiness measure.

**JOARDER KAMRUZZAMAN** (Senior Member, IEEE) is currently a Professor with the School of Science, Engineering and Information Technology, Federation University Australia. Previously, he has served as the Director for the Centre for Multimedia Computing, Communications and Artificial Intelligence Research hosted first by Monash University and later by Federation University Australia. His research interests include the Internet of Things, machine learning, and cybersecurity. He has published over 250 peer-reviewed publications and received Best Paper Award in four international conferences. He also received nearly A$2.4m research funding, including prestigious Australian Research Council and large Collaborative Research Centre grants. He has also served many conferences in leadership capacities, including a Program Co-Chair, a Publicity Chair, a Track Chair, and a Session Chair, and since 2012 as an Editor of the Elsevier *Journal of Network and Computer Applications*, and had also served as the Lead Guest Editor for Elsevier *Journal Future Generation Computer Systems*.

**ALIREZA JOLFAEI** (Senior Member, IEEE) received the Ph.D. degree in applied cryptography from Griffith University, Brisbane, QLD, Australia. He is currently the Program Leader of Master of IT in Cybersecurity with Macquarie University, Sydney, NSW, Australia. Before Macquarie University, he worked as a Lecturer with Federation University Australia, and as an Assistant Professor of computer science with Temple University, Philadelphia, PA, USA. He has participated in several projects involving different aspects of cybersecurity. On these topics, he has published over 100 articles appeared in journals, conference proceedings, and books. His research interests include cyber and cyber-physical systems security. He received multiple awards for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He also received the prestigious IEEE Australian council award for his research articles published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He has served as the Chairman of the Computational Intelligence Society in the IEEE Victoria Section and also as the Chairman of Professional and Career Activities for the IEEE Queensland Section. He has also served as a Guest Associate Editor for IEEE journals and transactions, including the IEEE INTERNET OF THINGS (IoT) JOURNAL, IEEE SENSORS JOURNAL, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRY APPLICATIONS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE. He has also served as a General Co-Chair, a Program Co-Chair, a Track Chair, a Session Chair, and a Technical Program Committee member, for major conferences in cybersecurity, including IEEE TrustCom and IEEE INFOCOM. He is also a Distinguished Speaker of the Association for Computing Machinery on the topic of cybersecurity.

**RAJKUMAR DAS** received the B.Sc. and M.Sc. degrees in computer science and engineering (CSE) from the Bangladesh University of Engineering and Technology (BUET), Bangladesh, in 2011 and 2008, respectively, and the Ph.D. degree in computer science from Monash University, Australia. He worked as an Assistant Professor of CSE with BUET. Being a Data Enthusiastic, he developed a string an end-to-end knowledge in data-space that includes advanced data analytics, data science, big data engineering, and machine learning. In his Ph.D. research, he developed data analytics framework to predict public opinion in online social networks. His current research interests include ITS, the IoT, and cybersecurity.