IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 4 September 2022, accepted 3 October 2022, date of publication 12 October 2022, date of current version 18 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3213843

TOPICAL REVIEW

Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art

PRINKLE SHARMA[1] AND JAMES GILLANDERS[2]

[1]Department of Information Security and Digital Forensics, University at Albany-State University of New York, Albany, NY 12222, USA
[2]Department of Informatics, University at Albany-State University of New York, Albany, NY 12222, USA

Corresponding author: Prinkle Sharma (psharma2@albany.edu)

This work was supported by the State University of New York-University at Albany.

ABSTRACT Connected Autonomous Vehicles (CAVs) are transformational technologies that have demonstrated significant potential for shaping the future of transportation systems. CAV research has been conducted extensively, both in academic and industrial pursuits. The intention was to put CAVs on the road, but the safety and efficiency of CAVs must be prioritized for this purpose to come to fruition. This technology is built upon sensors, and network communications have the potential to improve automotive infrastructure, reduce traffic and accidents, and facilitate a unified transportation system. Although the auspiciousness of these vehicles is clear, persistent threats exist in terms of cybersecurity attacks, which jeopardize the safety and effectiveness of CAVs. Our study provides a comprehensive dissection of cyberattacks and digital forensics on CAVs. We begin by discussing each element of a standard CAV network and then illustrate the current security. The three main components of CAVs– *sensors, communication networks, and actuators*-were analyzed in detail. The expansion of cybersecurity and forensic issues is presented with additional investigations into traditional and artificial intelligence-based cyber-defense techniques. Our work concludes by discussing the open challenges and potential research areas for developing robust cybersecurity and forensic solutions exclusively for CAVs.

INDEX TERMS Connected autonomous vehicles, cyber attacks, and forensics, cyber-physical systems, intelligent transportation system.

I. INTRODUCTION

Connected Autonomous Vehicles are gradually preparing consumers for when they will relinquish partial or full manual control of their vehicles. Several prominent corporations worldwide are already developing and testing their prototypes on roads [1]. Even though driverless cars hover around the advanced testing stage, partially automated technology has been around for half a decade and is present on roads today [2]. CAVs rely on several sensors, such as radar, LiDAR, and cameras, to survey the driving environment in real-time and notify the occupant of any immediate threat or hazard. CAV actuators, such as throttle, steering, and braking, enable the system to react accordingly after receiving information from the sensors. For example, the radar sensor notices an object on the road, prompting the vehicle to switch lanes and avoid collisions. With the rapid advancement of CAV technologies, the transportation industry is inching toward an era of full autonomy, as defined in SAE J3016 [3]. Original equipment manufacturers s (OEM) optimizes their vehicle's software with updates to keep their systems up to date. Many current CAVs offer level 2 autonomous vehicle features, including automatic cruise control, hazard warnings, and emergency braking. Despite e these technological improvements, cyber-attacks have become a major threat to the intelligent transportation systems (ITS) of CAVs [4]. Although millions of investments are being made to improve CAV robustness and safety, security compromises continue to increase. There have been several real instances, such as the death of two passengers driving a Tesla by hitting a semi-truck in Florida in July 2022 [5], and the death of a bicycle on the road at night in Arizona when hit by an

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

Uber self-driving car [6]. These incidents indicate that CAV manufacturers and systems have a long way to go before earning the trust they desperately need.

To create a reality that autonomous vehicle manufacturers desire and operate effectively, vehicles must be outfitted with state-of-the-art sensory and communicative capabilities. Concerning the feasibility of an attack and its fatal effects on CAV sensors, onboard units, and infotainment systems, communication networks will need to provide insights into spotting vulnerabilities in the system's defenses.

This study primarily focuses on discussing cybersecurity, forensics, and defense mechanisms of CAVs. Cybersecurity and forensics in CAVs as two essential sides of the same coin - the work they do is very similar but differs in a few key ways. Cybersecurity is a preventive function, and forensics is a detective function; in other words: the cybersecurity team works to implement and maintain a robust information security system, to defend the systems from cyber-attacks; in the case that their efforts fail, and an attack is made, the forensics team works to identify the hack, understand the source, and recover compromised data by tracing the digital footprints of the attacker.

The remainder of the paper is organized as follows: Section II discusses our broader research contributions and analyzes existing work on cybersecurity CAV forensics, considering information or topics that may be missing in their work. Section III presents the architectural context of connected autonomous vehicles in an Intelligent Transportation System (ITS). The security and forensic standards for connected autonomous vehicles are discussed in Section IV. Section V highlights the challenges of cybersecurity and forensics in CAVs. Section VI provides a survey review of existing solutions to cyberattacks and forensics in CAVs, transitioning to Section VII, where we discuss the open challenges in ITS development. Finally, Section VIII concludes the paper by concluding our thoughts and future research.

II. CONTRIBUTION

Analyses of sensors and cybersecurity in connected autonomous vehicles reveal the underlying principle of CAV technology, that is, the coagulation of human passenger and automated transportation. Thus, explaining each sensor, communication network medium, potential cyberattacks/countermeasures, and their contribution to the safety of vehicular networks are necessary. As mentioned in [7], there has been a noticeable increase in the number of survey papers published on cybersecurity and forensics in CAVs; however, most studies analyzed cyberattack risks and vulnerabilities; moreover, only a few dig into the topic of forensics. In addition, several studies [8], [9], [10], [11], [12], [13] have proposed novel defense strategies against cyberattacks, but none that we have come across in all our research provide a singular robust solution to safeguard CAVs from cyberattacks. Furthermore, the surveys listed do not discuss security standards and their relationship to cyberattacks and forensics, which are significant aspects of any CAV's defense.

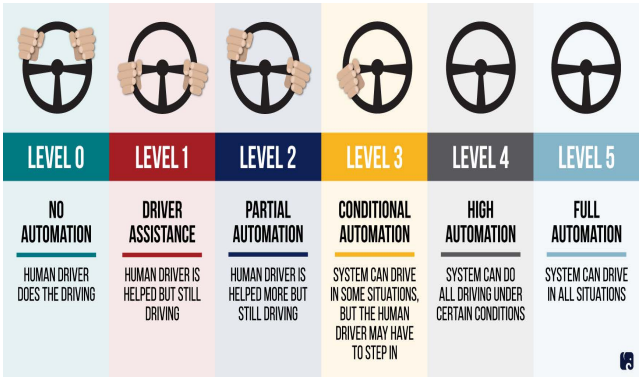

FIGURE 1. Levels of autonomy in vehicles [14].

This study seeks to bridge the gap by addressing:

(i) Providing an overview of the complete Intelligent Transportation System

(ii) List of current safety and forensics standards in Intelligent Transportation System

(iii) Current cybersecurity and forensics challenges in CAVs

(iv) Existing cyber defense solutions based on traditional and artificial intelligence techniques

(v) Discussion on open research challenges in CAVs

III. CONNECTED AUTONOMOUS VEHICLES OVERVIEW

Generally, CAVs can connect, share, and interact with other intelligent vehicles (CAVs) and their environment via their sensors and an onboard unit that operates according to standardized protocols. As shown in Figure 2, the three critical elements of CAVs are (i) Autonomous Driving Systems, (ii) Connected Driving Systems, and (iii) Intelligent Transportation Systems, all of which are explained in detail below.

A. AUTONOMOUS DRIVING SYSTEMS

An *Autonomous Driving System* was built to sense an environment via sensors and operates without any human intervention (mostly). The system connects the vehicle's sensors, ECUs, and actuators to other components in the vehicle, forming an autonomy stack that allows for data compilation, decision-making, and taking action. Sensors perceive the surrounding environment and process related data, such as the distance between objects. Subsequently, the autonomy stack collects sensor data and makes decisions accordingly. Finally, the vehicle's actuators (throttle, steering, and brake) make executive decisions by delineating instructions to adjust the vehicle's physical behavior. As defined by the Society of Automotive Engineers (SAE) J3016 [3], there are several levels of Autonomous Driving Systems, and in the real world, we are just getting started. Six levels of driving automation have been introduced, ranging from no to full automation. Figure 1 illustrates the level of automation:

1) **No Automation (Level 0):** Driver fully controls the vehicle

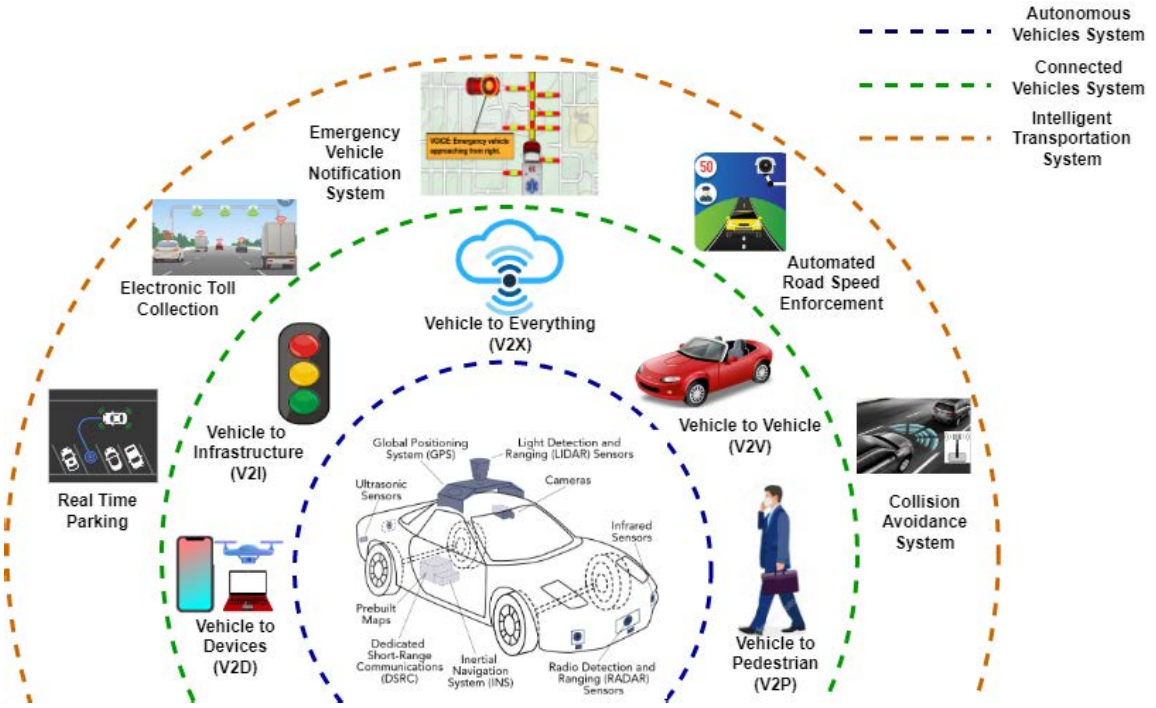

FIGURE 2. Overview of connected automated system vehicle infrastructure.

2) **Driver Assistance (Level 1):** Minor driving tasks performed by automation such as adaptive cruise control
3) **Partial Automation (Level 2):** The driver must stay alert and actively supervise the driving via the Advanced Driving System and should be able to take over steering, acceleration, and braking in specific driving scenarios.
4) **Conditional Automation (Level 3):** The driver does not need to be fully alert and oversee driving tasks, meaning they can engage in other activities. However, the driver must be ready to perform manual control in an emergency. Technologies such as traffic jam assistance are present at this level of automation.
5) **High Automation (Level 4):** Drivers are not required for specific use cases. In such scenarios, the vehicle may not have a steering wheel and pedals but will be restricted to particular geographic boundaries using geofencing technology. Certain conditions, such as severe weather, may temporarily limit or cancel the vehicle operation. For example, driverless taxis and public transportation are at this level of automation.
6) **Full Automation (Level 5):** The highest level of automation in vehicles where no human interaction is required, and a car can drive itself everywhere in all conditions.

Autonomous Driving Systems rely on several sensors, actuators, algorithms, machine-learning systems, and powerful processors to operate vehicles effectively. The most common sensors in Autonomous Driving Systems are ultrasonic sensors, LiDAR, cameras, encoders, inertial sensors, and global navigation satellite systems (GNSS). These sensors can be further classified into two classes based on their functions. An *external sensor* is a perceptual sensor that manages the external state of a vehicle by sensing its external environment. The *Internal sensor* is more analytical, mainly containing the internal states of the car, and it processes the data received by the vehicle. The operation of each sensor is discussed below:

1) CAMERA

The most widely adopted sensor technology for Autonomous Driving Systems, which boasts the ability to distinguish various environments and targets, cameras are becoming widely implemented even in manually controlled vehicles. Several cameras have been integrated with sensory technology, such as depth-of-field, RGB, DVS, and optical flow. Cameras and vehicle-incorporated software can detect both moving and static obstacles, including road signs, emergency vehicles, traffic lights, pedestrians, and other visual stimuli that a human can identify. CAV cameras operate based on the landing light emitted from objects on a photosensitive surface through a lens [15]. There are many types of cameras depending on the lens type (i.e., wide-angle for near-field and narrow-angle for far-field applications) or the parts of the spectrum they cover, such as night vision (NV) or specialty chips such as High Dynamic Range (HDR) which are extremely sensitive to light. High-resolution cameras, such as infrared cameras, outperform human eyes because they can detect specific wavelengths in the spectral range of 0.9-1.7 microns. Cameras are essential for automated vehicles.

However, they are heavily affected by low-light weather conditions and require extensive computational processing to extract the data.

2) LiDAR

Light Detection and Ranging (LiDAR) technology is used to locate objects on roads and measure their distance. It operates based on the principle of emitting laser light pulses that reflect from a target object. The time interval between the emission and reception of the light pulse back to the sensor is used to calculate the distance [16]. Using shorter-wavelength laser light helps achieve a higher measurement accuracy and spatial resolution. The distance was estimated at a clocking speed of 150 kHz, and the ability to chart the navigational environment using LiDAR was instantaneous. LiDAR scans its surroundings and generates a three-dimensional (3D) representation of the scene as a point cloud. Currently, 3D spinning LiDARs are more commonly used to ensure reliable perception under any light condition (day or night) [16]. Issues with LiDAR technology include high manufacturing costs and vulnerability to cyberattacks; however, newly optical phased array LiDAR technology [17] has demonstrated success in meeting the performance and cost requirements of the AV market. Additionally, unlike cameras, LiDAR sensors do not generate information about their surroundings in color and require data fusion with other sensors to make decisions.

3) RADAR

or Radio detection and ranging, is used to detect objects at a distance and gauge their speed and characteristics. It consists of a transmitter, receiver, receiving antenna, processor, and radio-wave transmission and reflection techniques to estimate the distance from the target object. The time required for a radio wave to travel forward and backward is determined by the distance between the radio wave source and the target object that reflects the radio waves, similar to LiDAR. Although some differences between radar and LiDAR devices are that radar uses radio waves with an antenna, while LiDAR devices have specialized optics and lasers for receiving and transmitting. Second, the radar can detect the distance of a target object rather than its actual appearance, as opposed to LiDAR, which can detect and locate a target object. Lastly, (iii) radar works in overcast weather conditions and at night, but neither LiDAR nor camera offers these features on their own.

4) ULTRASONIC

Similar to certain living organisms that use echolocation, ultrasonic sensors emit sound waves to process the distance between themselves and nearby objects. Ultrasonic sensors are interior sensors that work alongside other sensors, such as radar, cameras, and LiDAR, to paint a complete picture of any surrounding vehicles. In general, ultrasonic sensors perform best when detecting proximity and slow speeds. However, they also function well under fog, severe weather, and low-light conditions. These sensors are generally the cheapest of all the sensor types discussed thus far; however, unlike LiDAR, they do not have the resolution to detect small or multiple objects moving at high speed. These sensors best detect solid hazards such as traffic cones and barriers.

5) WHEEL ENCODER

A wheel encoder was attached to the wheels of the vehicle to measure the rotation and observe the velocity and acceleration of the car. An internal sensor coupled to the steering wheel of a vehicle captures the angle of turn.

6) INERTIA MEASUREMENT UNITS

An Inertia Measurement Unit (IMU) sensor operates by ensuring angular rate, force, and magnetic field. It consists of two sensors: an accelerometer and a gyroscope, which measure linear and rotational acceleration. The sensor is independent of the visual or radio spectrum information and is installed in a shielded container inside the vehicle's chassis; therefore, it is entirely immune to weather and other environmental conditions and supplies real-time data from all six-axis movements simultaneously. This navigation sensor will also help automated cars stabilize themselves and determine whether they should take any protective safety action (e.g., deploy an airbag, prevent the vehicle from rolling over, etc.).

7) GLOBAL NAVIGATION SATELLITE UNITS

The Global Navigation Satellite Units (GNSS) sensors can be used to navigate vehicles from points A to B. This sensor works along with the GPS of the CAVs to determine a location's latitude and longitude with assistance from satellite transmissions. The user interface can emulate existing GPS systems, requiring minimal human input because the vehicle does the rest. Regarding technological aspects, a GPS tracking system uses a GNSS network to communicate with satellites. In contrast, GNSS uses microwave signals transmitted to GPS devices to provide information on location, speed, time, and direction necessary for practical, automated driving.

Actuators are another essential component of Autonomous Driving System technology integrated into CAVs. Once the data are received from the environment via sensors, the vehicle's Electronic Control Unit (ECU) determines the activation of the actuator. Actuators operate behind the scenes within vehicles to convert energy into reality. They perform various convenient functions, including backup cameras, blind spot monitoring, lane assistance, emergency braking, and adaptive cruise control [18]. Currently, most vehicles on the road already have actuators (described below) required for autonomous vehicles.

- **Throttle Actuator** - Pressing or releasing the gas pedal to control the vehicle's speed via electronic control.
- **Steering Actuator** - Controlling the direction of the vehicle via electrically assisted power steering.

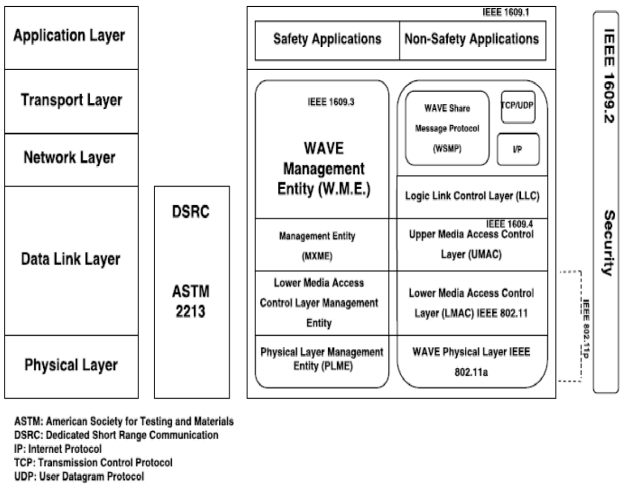

FIGURE 3. Protocol stack [19].

- **Braking Actuator** - Deciding when to stop a moving vehicle via electronic stability control.

B. CONNECTED DRIVING SYSTEMS

Connected Driving System technology connects the vehicle's vehicle and roadside infrastructure (traffic lights, roadside units, pedestrians, drones, etc.) within the network of intelligent transportation systems. It allows them to communicate bidirectionally within a 300-meter range. The broadcast includes vehicle credentials (longitude, latitude, speed, heading, etc.), safety warnings, weather, and traffic congestion details that determine safety, mobility, and driving experience. The data within the connected network are meant to be broadcast anonymously. That is, the communicating devices cannot be tracked. This technology is based on various standards included in the DSRC protocol stack (Figure 3), which are primarily based on the IEEE 802.11p and IEEE 1609 standards. Below, we explain each criterion in detail:

- **SAE J2735 Dedicated Short Range Communication:** Dedicated Short Range Communication (DSRC) technology is built off the IEEE 802.11p standard, which allows highly secure and direct communication between vehicles inside an Intelligent Transportation System to communicate with other devices. The DSRC uses the 75 MHz bandwidth of the spectrum in the 5.9 GHz band provided by the United States Federal Communication Commission in 2004. It is designed to achieve low latency and high reliability within connected vehicles without a cellular network. This standard ensures functional features, including collision avoidance, emergency vehicle warnings, and signage in the network [20].
- **SAE J2945/1 Onboard Minimum Performance Requirements for Safety Communications:** This standard sets the minimum system performance requirements for an on-board vehicle-to-vehicle (V2V) safety communication system for light vehicles, including standard profiles, functional requirements, and performance requirements [21].
- **IEEE 802.11p protocol:** IEEE 802.11p is an amendment of the IEEE 802.11 standard to include Wireless Access in Vehicular Environments (WAVE). The connected driving system not only requires a reliable wireless connection but also requires high speed. Because communication between devices will exist only for short time intervals, there will not be sufficient time to perform the usual authentication procedures. IEEE 802.11p defines a method to enable the exchange of data between devices by including a wildcard BSSID in the header of the frames with which they communicate and exchanging data frames when they arrive in the communication channel [22].
- **IEEE 1609 Standard for Wireless Access in Vehicular Environments (WAVE):** This protocol defines the structure of the IEEE 1609 family and is specifically designed for vehicular networks. IEEE 1609 families, along with IEEE 802.11p, describes the architecture, communication models, management structures, security mechanisms, and physical access for high-speed short-range wireless communications within vehicles' on-board and roadside units [23].
- **IEEE 1609.1 Network Resources Management:** The IEEE 1609.1 protocol describes the data and management of services offered within the WAVE. It specifies the data flows, resources, fundamental components, device types supported by vehicles, command messages, and storage formats [23].
- **IEEE 1609.2 Security Services for Applications and Management Messages:** The IEEE 1609.2 protocol provides security services to avoid malicious users and attacks on the vehicular network. This security service uses security data stores (SDSs) to support security-related information, including the current time, location, and source of random numbers that security services need to perform security operations [23].
- **IEEE 1609.3 Networking Services:** The protocol defines network and transport layer services, including addressing and routing to support secure data exchange in WAVE. It also defines WAVE short messages and the Management Information Base [23].
- **IEEE 1609.4 Multi-Channel Operations:** This protocol supplies enhancements to IEEE 802.11 Media Access Control to support WAVE operations and describes various standard message formats for DSRC [23].

There are distinct types of connected communication technologies available, and automotive and information technologies work hand in hand. Below, we discuss the general types of connectivity technology:

1) VEHICLE TO VEHICLE (V2V)

The V2V communication system allows data transmission between vehicles by broadcasting it in real-time. This includes exchanging information wirelessly, such as the

speed, heading, and position of the surrounding cars, to avoid crashes, ease traffic congestion, and improve the driving environment. The V2V technology in vehicles communicates via Basic Safety Messages, A.K.A. BSMs, which have a range of approximately 300 meters (best-case scenarios) and promptly broadcast information at a rate of 10Hz. Information broadcasts via BSMs allow vehicles to operate safely and efficiently.

2) VEHICLE TO INFRASTRUCTURE (V2I)

A vehicle for the infrastructure communication system was built to enhance vehicle safety. vehicles communicate with road infrastructure via Road Side Units (RSUs) and share/receive information such as traffic/road/weather conditions, speed limits, and accidents. Connectivity is used for bidirectional communication through hardware, software, and firmware to support systems such as lane signs, road signs, and lighting systems. This technology warns drivers of collisions, jams, fast curves, and speed. V2I technology will also enhance driver-assistance methods, such as parking and automatic toll payments, which could further assist in planning smart city traffic lanes and parking lots.

3) VEHICLE TO EVERYTHING (V2X)

Vehicle to everything is the communication between a vehicle and any device that could be affected by the vehicle's information on the road. The main purpose of V2X technology is to enhance safety, save energy, and make traffic on the road more efficient as part of an intelligent transportation system. The key components of the V2X technology are V2V and V2I. When V2X systems are integrated into traditional vehicles, drivers can receive essential information regarding weather patterns, nearby accidents, road conditions, road work warnings, approaching emergency vehicles, and the activities of other drivers on the same road.

4) VEHICLE TO PEDESTRIAN (V2P)

Vehicle to Pedestrian communication networks provides direct communication between vehicles and pedestrians. The scope of the V2P also applies to cyclists. The signals are transmitted from the smartwatch to the onboard unit if any of the pedestrians are within the range of connected vehicles. Similar to V2V, safety messages, including speed, location, and heading information from pedestrians, are broadcast to approaching vehicles and vice-versa. Depending on the frequency of the V2P, it can send a maximum of 10 alerts per second.

C. INTELLIGENT TRANSPORTATION SYSTEMS

The ITS is an application that aims to supply services related to transportation and traffic management services to make driving smarter, safer, and more coordinated. Figure 4 shows the taxonomy of the Intelligent Transportation System. The system aims to deliver real-time information, including travel time, speed, delay, road accidents, route changes, diversions, and work zone conditions. The ITS relies heavily on data collection and analysis via sensors. Decision-making is performed after analyzing the data exchanged among vehicles, transport infrastructure, and pedestrians. Sensor deployment within the transportation network provides drivers with new services such as smart parking, electronic toll collection, and reduced pricing according to congestion levels on the road. Road sensors collect environmental data in real-time, which are then processed and analyzed to improve transportation networks and make them resilient [25]. As described in [26], sensors in ITS can be classified into two categories based on their location: intrusive and non-intrusive. Interior sensors were installed on road pavement surfaces. They have high vehicle detection accuracy but high installation and maintenance costs. Non-intrusive sensors are installed at different locations in the infrastructure (not road pavement) to detect a vehicle's speed, direction, and lane coverage. However, they are expensive and affected by environmental conditions. Table 1 provides an overview of road sensors and their functioning in an Intelligent Transportation System. The authors recommend the reader for an in-depth study of road sensors [24]. Some applications of Intelligent Transportation Systems include the following:

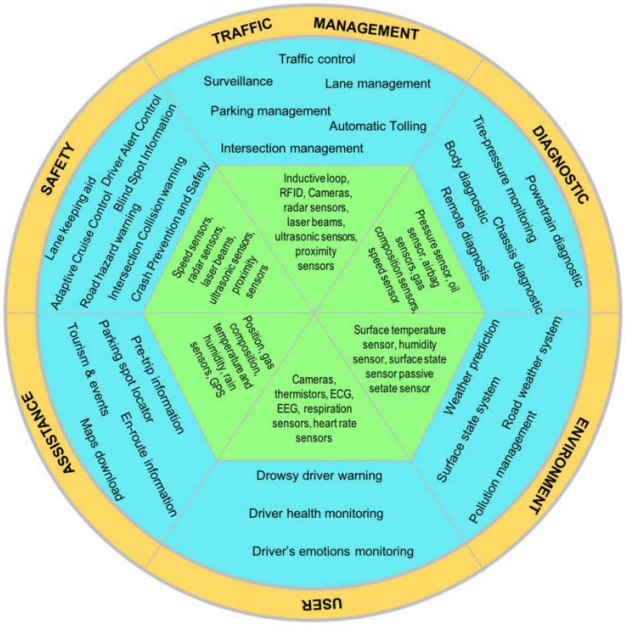

FIGURE 4. Taxonomy for ITS applications [24].

- Real-time Parking Management
- Electronic Toll Collection
- Emergency Vehicle Notification Systems
- Automated Road Speed Enforcement
- Speed Alerts
- Collision Avoidance Systems
- Dynamic Traffic Light Sequence
- RFID in Freight Transportation

IV. CURRENT SECURITY AND FORENSICS STANDARDS

CAVs require continuous, real-time, wireless connectivity to communicate between users, sensors, and devices. Therefore,

TABLE 1. Summary of sensors in intelligent transportation systems [24].

Category	Sensor Type	Application and Use
Intrusive	Pneumatic Road Tube	Used for keeping track of the number of vehicles, vehicle classification, and vehicle count.
	Inductive Loop Detector (ILD)	Used for detecting a vehicle's movement, presence, count, and occupancy. The signals generated are recorded in a device at the roadside.
	Magnetic Sensors	Used for detection of the presence of vehicles, identifying stopped and moving vehicles.
	Piezoelectric	Classification of vehicles, counting vehicles and measuring vehicle's weight and speed.
Non-Intrusive	Video Cameras	Detecting vehicles across several lanes can classify vehicles by their length and report vehicle presence, flow rate, occupancy, and speed for each class.
	Radar Sensors	Vehicular volume and speed measurement, detection of direction of motion of the vehicle, and used by applications for managing traffic lights.
	Infrared	Application for speed measurement, vehicle length, volume, and lane occupancy.
	Ultrasonic	Tracking the number of vehicles, vehicle presence, and occupancy.
	Acoustic Array Sensors	Used in developing applications for measuring a vehicle's passage, presence, and speed.
	Road Surface Condition Sensors	Used to collect information on weather conditions such as the surface temperature, dew point, water film height, road conditions, and grip.
	RFID (Radio-frequency Identification)	Used to track vehicles mainly for toll management.

ensuring crash prevention, safety, and mobility is crucial. Any network should satisfy traditional security requirements, including:

- **Availability:** Collected information should always be available to devices in the network so that timely decisions can be made.
- **Authorization:** Only legitimate and authorized sensors and communication networks have the right to collect and distribute information to other devices and environments.
- **Confidentiality:** Information shared should be encrypted and should only be available to authorized devices n the network.
- **Integrity:** Broadcasted/Shared information should not be changed or forged.
- **Privacy:** Collected information should not be shared with any other entity or organization without permission.

In the following section, we discuss existing standards and protocols available for connected autonomous vehicles.

A. SECURITY STANDARDS

The number of connected devices is increasing, and so are the vulnerable threat points for hackers. Cyberattacks pose severe concerns to the automotive industry because they directly affect driver safety and data privacy. Below, we describe the existing standards for wireless access technology that can be applied to connected autonomous vehicles.

1) **ISO/SAE 21434:** The ISO/SAE 21434 standard helps the industry to define a structured process that ensures that cybersecurity is incorporated into road vehicle design, - including systems, component software, and connections to any external device or network. The standard focuses on cybersecurity fundamentals, including requirements, processes, and goals in business disciplines, such as product development, construction, operations, and maintenance [27]. The standard considers the entire development process and life cycle of a vehicle [27]. It supports *Security by Design* processes and includes phases ranging from engineering, design, specification, implementation, testing, operations, and security. All the phases included in ISO/SAE 21434, make this standard one of the most comprehensive approaches to connected vehicle cybersecurity [28].
2) **The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29):** The WP.29 standard adopted in June 2020 is a new international automotive cybersecurity regulation that paves the way for connected vehicles and mitigates any cybersecurity risks posed to passenger vehicles. This regulation sets up the performance and audit requirements for the cybersecurity and software update management of new passenger vehicles. It includes three phases: development, production, and post-production, which comprise monitoring, detecting, and responding to cyber-attacks [29]. The standard requires automakers to implement measures to [29]:
   - Manage vehicle cybersecurity risks
   - Secure vehicles by design to mitigate any risks along the supply chain
   - Detect and respond to security incidents across the vehicle fleet
   - Provide safe, secure software updates and do not compromise vehicle safety
3) **SAE J3061:** The cybersecurity guidebook for cyber-physical vehicle systems was developed by the SAE International Association of Engineers and Technical Experts in the aerospace, automotive, and commercial vehicle industries. The standard aims to provide guidelines concerning cybersecurity in cyber-physical systems applicable to any organization. The standard is based on many existing studies on security engineering and secure system development methodologies and is strongly related to the automotive system functional safety standard ISO 26262 [30]. J3061 divides the lifecycle into five processes: concept phase, product development, production, operation, and service. The goal of the concept phase is similar between ISO 26262 and J3061, but there are differences between Hazard Analysis and Risk Assessment (HARA) in ISO 26262 and TARA in J3061 [30]. HARA focuses on identifying and categorizing malfunctions in an item that can lead to a hazard, whereas TARA focuses on threats to a feature.

B. FORENSIC STANDARDS

Connected Autonomous Vehicles rely on onboard sensor computations on roads, with limited or no human intervention. However, decision-making in CAVs could go wrong for one or many reasons, which could lead to mishappenings. Currently, CAVs lack a concrete forensic investigation framework/standard that is needed to resolve issues including insurance disputes, investigating attacks, and CAVs driving compliance safety guidelines. As of May 2022, the National Institute of Standards and Technology (NIST) has not released any standards or guidelines for investigating incidents involving CAVs, even though they have started initiatives through workshops [31], in which they currently focus on a broader perspective of standards and performance metrics for CAVs. NIST has released hundreds of tools in the *Computer Forensic Tools and Techniques Catalog*.[1] However, only one tool targets passenger vehicles, which is incompatible with CAVs. The only forensic standard available for handling digital data is *ISO/IEC 27037*. The standard provides regulations on handling digital evidence, which includes the identification, collection, acquisition, and preservation of potential digital evidence that can be helpful in court.

To design robust and secure CAVs, it is crucial to determine the reasons for accidents and mishappenings involving them. Therefore, it is essential to collect logs from different artifacts of CAVs and store them in a tamper-proof manner. Theoretically, as shown in Figure 5, forensics can be performed in two ways: **Reactive** and **Proactive**. The *reactive approach* is the traditional (or post-mortem) approach to investigating digital crimes after an incident has occurred. This involves finding, preserving, collecting, analyzing, and generating a final report. Figure 6 shows a generalized reactive forensic approach for automotive forensics. Two types of evidence were collected using a reactive forensic approach:

- **Static:** This approach refers to collecting all the static impedance remaining after an occurrence, such as the graphic of a hard drive.
- **Dynamic:** Collecting all live (dynamic) evidence present after an occurrence.

The *proactive forensic* approach works to proactively collect data, protect it, detect dubious events, gather facts, conduct research, and build a case against any questionable activities. The evidence gathered using this forensic approach includes information related to a particular event or incident. The phases of the proactive components are as follows:

- **Proactive Collection:** Live collection of pre-defined data in order of volatility and priority.
- **Proactive Preservation:** Automated preservation via evidence hashing and proactive collection of data related to suspicious events.
- **Proactive Event Detection:** Detecting any suspicious event via forensic investigation tools.

[1] https://toolcatalog.nist.gov/

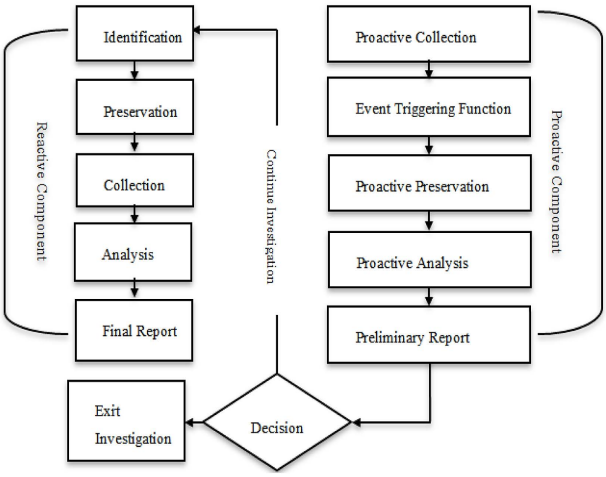

FIGURE 5. Functional process for proactive and reactive digital forensics investigation system [32].

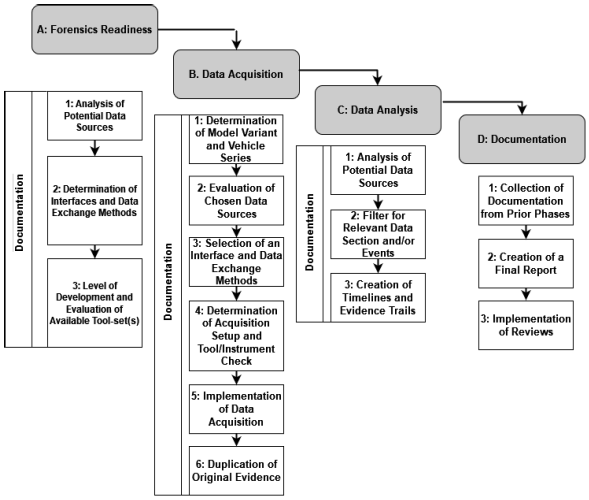

FIGURE 6. Autonomous vehicles forensics model [34].

- **Proactive Analysis:** Automated live analysis of the evidence, that could be used to construct the first hypothesis of the incident.
- **Report:** Automated report generated from the part analysis. It is an important part of forensics and serves as a starting point for reactive investigations.

Several digital forensic investigation frameworks have been proposed in the literature, and most agree that the fundamental principles of digital forensic investigations are **Reconnaissance**, **Reliability**, and **Relevancy** [33]. The investigator was required to ask questions related to the event, including what, who, how, when, why, and where. These questions can incorporate investigators, legal advisors, and prosecutors into a bigger picture of the investigation, while also exploring the opportunities for reconnaissance, evaluating the reliability of the information and method, and showing the relevance of the event to the investigation. Therefore, both proactive

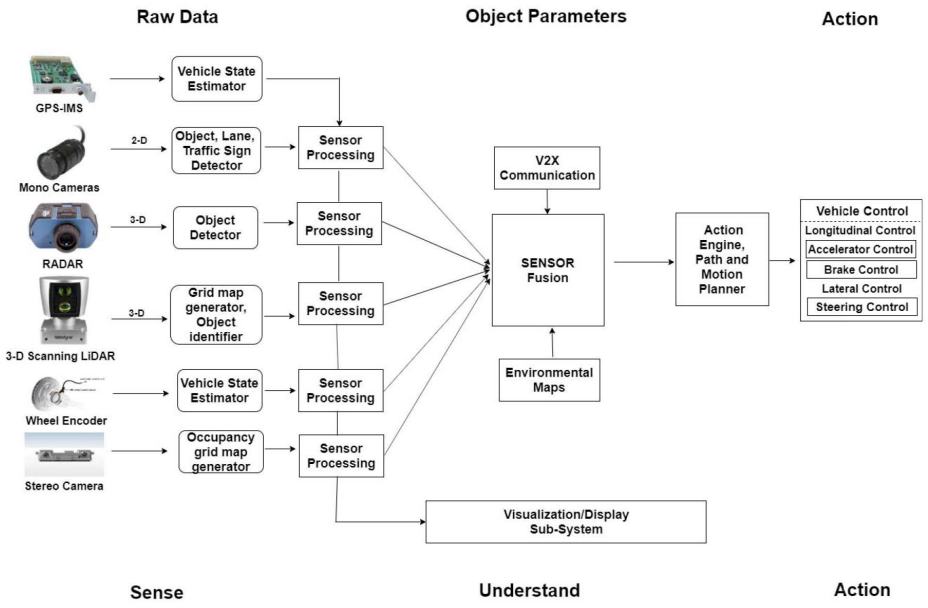

FIGURE 7. Connected autonomous vehicle data fusion [35].

and reactive approaches should focus on data collection and reporting to describe the events.

V. CHALLENGES IN SECURITY AND FORENSIC

Cybersecurity and defense against attacks are legitimate possibilities in sensory technology, and connected autonomous vehicles are no exception. Although there is limited research, testing has been performed against attacks not only in CAV but also in sensory technology. Figure 7 shows the lifecycle of CAVs, including the autonomy, connectivity, and fusion of data by sensing the environment via sensors, collecting data from multiple sources, and fusing them to take the necessary action via actuators. Below, we classify security attacks on CAVs into three categories:

A. PART 1.1: SENSOR SECURITY ATTACKS

To drive autonomously and safely, CAVs must perceive their surroundings by using sensors. Sensors rely on computer-enabled object-based detection, which helps CAVs find an object, label it, and decide its action. However, the problem is that the sensors technology has a long way to go before it can aid CAVs with decision-making to drive safely on the road. Sensor-based applications are highly vulnerable to cyberattacks and can lead to disruption, disabling, destroying, or maliciously controlling a CAV/environment, or destroying the integrity of data. The threats to the sensing layer in CAVs include (are not limited to):

1) **Spoofing Attacks:** Spoofing attacks are performed when an attacker pretends to be someone or something else that appears to be associated with a trusted/authorized source in the communication network. For CAVs, spoofing attacks can involve i) altering the distance between the source and receiver by injecting incorrect sensor data values. (ii) obtaining objects on the road, and (iii) injecting fake signals into the sensors. Researchers have demonstrated successful spoofing attacks using GPS, cameras, LiDAR, ultrasonic, and wheel encoder sensors in CAVs.
2) **Jamming Attacks:** A jamming attack is executed by an attacker in the network - to disrupt the transmission and reception of legitimate wireless signals among sensors. This type of attack can be launched by an attacker both internally and externally. The attacker uses a high-power transmitter called *Jammer* to interfere with the wireless network, thereby preventing the source sensor from either stopping the transmission or receiving legitimate data packets. Jamming attacks can occur on several sensors in CAVs including LiDAR [36], [37], Radar [38], Camera [36], and Ultrasonic Sensors [39].
3) **Tampering Attacks:** Tampering attacks occur when an attacker manipulates the data parameters exchanged between the sensor and the receiver without user authentication. The tampering can be performed in two ways: (i) Remotely, and (ii) Physically. Remote tampering can be performed either by placing stationary attacking equipment along the roadside unit or by manipulating the environment scenery, traffic lights, or road signs to deceive the vehicle's sensors. However, physical tampering requires an attacker to directly access a benign vehicle. The attacker attacks by physically damaging vehicle sensors or by placing materials that interfere with the sensor and vehicle control system [40], [41].

4) **Adversarial Attacks:** Adversarial attacks are performed using artificial intelligence techniques. The attack involves introducing adversarial examples into the sensor perception model and subtly modifying the original image such that changes are almost undetectable to the human eye. This could result in the misclassification of elements, such as road signs, and traffic lights. Several researchers have successfully performed adversarial sensor attacks on LiDAR [42], [43], cameras [44], Radar [45], and ultrasonic sensors [46].
5) **Denial of Service/Distributed Denial of Service Attacks:** Denial of Service or Distributed Denial of Service attacks in CAVs occur when an attacker injects an enormous number of fake objects created by jamming or spoofing attacks. When the number of injected signals is greater than the maximum number of objects that any sensor can track, the system becomes unstable and may result in life-threatening events. LiDAR [47] sensors are extremely sensitive to this type of attack.

B. PART 1.2: COMMUNICATION SECURITY ATTACKS

The communication layer in CAVs handles the connectivity and routing of messages among the devices. The communication layer defines how the connection is proven to exchange data between devices, and how they are stored in the cloud. Cyber threats to the *communication layer* include sending incorrect details in messages, gaining control of the vehicle through infotainment systems, and eavesdropping on messages shared between devices. Below, we discuss, in detail, the types of attacks (not limited to) that could occur in the communication layer:

1) **Sybil Attacks:** Victim of this type of attack usually involves scenarios in which reputation is a major aspect. The attacker creates many pseudonyms identities in the system and uses them to gain maximum influence. Based on this influence, the attacker misleads other devices in the system for personal benefit, including diverting the traffic to get the road to itself, creating accidents by sending incorrect location/speed information, and creating illusion scenarios for vehicles on the road [48]. This is one of the most serious communication attacks as the attacker claims to be at a different geographical location at the same time [49].
2) **Replay Attacks:** Replay attacks are performed when an attacker hijacks and records the signals transmitted by the sensor(s) without user knowledge. The attackers then conduct a replay attack by sending the recorded signals back to the sensor(s) to cause the sensor(s) to map non-existent objects. LiDAR [42], [47], [50]
3) **Relay Attacks:** Relay attacks are an extension of replay attacks that typically involve two people working together. The attacker receives the signals transmitted by the sensor(s) and forwards them to the receiver at different locations. The receiver then re-sends the signals back to the original sensor(s), resulting in an incorrect object location map. Some successful studies on relay attacks are included in [51].
4) **Remote Attacks:** Remote attacks refer to attacks performed in a network without any physical contact with devices. In such attacks, remote attackers search for vulnerable points in device/network security to ensure the system is remote, steal data information, and/or create accidents. In CAVs, remote attacks generally occur through a vehicle infotainment system [52]. A few previous studies demonstrating successful sensor remote attacks include [36], [53], [54], [55]
5) **Malware:** Malware attacks are common cyberattacks in which malware executes unauthorized actions on a victim's system [56]. This includes the introduction of ransomware, spyware, and viruses into a network system [57].
6) **Impersonation Attacks:** In an Intelligent Transportation System, every device has a unique identification number, which helps recognize the vehicle and messages transmitted. An impersonation attack occurs when an attacker uses the identity of another vehicle to steal information or gain control over a device [58]. In the case of CAVs, the attacker can impersonate the RSUs to trick the connected devices in the network to share their authentication detail, and then use the information to perform malicious activities.
7) **Data Falsified Information Attacks:** This type of attack occurs when an attacker broadcasts/sends incorrect information for personal gain [59]. Misleading information can create issues such as communication congestion, increased travel time, and imbalance in the usage of transportation resources.
8) **Man-In-The-Middle Attacks:** These attacks pose a serious threat to network security by either eavesdropping or altering the messages exchanged between two legitimate vehicles [60]. The exchanged information may contain sensitive and delay-intolerant information, such as emergency warnings, which could result in the dissemination of compromised and incorrect information throughout the network, thereby violating the main pillars of security and privacy requirements.
9) **Blackhole Attacks:** Dropping a data packet instead of sending it to its destination results in a black hole scenario where no data packet will move through to other devices in the network. These are also known as *Routing Attacks* [61]. Thus, we have *Greyhole attacks* in which only a small percentage of data packets are dropped to avoid detecting the attacker.

C. PART 1.3: ACTUATOR SECURITY ATTACKS

Action Engine aka actuators defines all applications where CAV technology has been deployed. Attacks deployed on sensors or communication networks directly (or indirectly) affect the functionality of action engine applications including automated steering control, lane change maneuvers, and braking status. These types of attacks are closely related to

sensor and *communication* attacks because they are mostly concerned with tampering with sensor information, communications, and decision-making mechanism using an Action Engine. Below, are the common types of attacks that target an action engine:

1) **Sensor Fusion Attacks:** Sensor fusion is the process of combining the input data from several sensors to predict a complete, correct, and dependable picture of a dynamic environment. Sensor fusion uses raw data from sensors, extracts the key features of the collected data, and then uses the information to make an informed decision. The process involves the fundamentals of machine learning models including statistical, probabilistic, knowledge-based, and reasoning-based methodologies. However, machine learning models, are vulnerable to attacks such as data poisoning, escape attacks, model stealing attacks, and model inference attacks [62].
2) **Piggybacking Attacks:** Applications and decision-making mechanisms are updated and installed via human intervention and automatic prompts. An attacker can change the source of software during the installation process, leading to a modified version of the software [63]. This manipulation may affect the capability and execution of ongoing processes.
3) **Supply-Chain Attacks:** Applications and decision-making mechanisms depend on third-party software and libraries that ease the functionalities required by software [64]. Any attack that affects the dependency of the software may have a critical impact on the action engine and change many CAVs [65].

Apart from the above-mentioned intentional attacks, CAVs are also prone to unintentional attacks caused by hardware and software failures/faults. This includes broken hardware wire connections, magnetic fields, non-functional or noisy sensors, and cosmic radiation. Such faults are difficult to differentiate from the above-mentioned attacks and require special investigation of data artifacts to discover the cause.

D. PART 2: CAVs FORENSICS CHALLENGES

As a complex system, CAVs impose several challenges, as they store a large amount of digital information, including personal data. The data are transferred via (i) buses for internal communication stored in the physical memory and (ii) the network for external communication stored in the cloud. Owing to the multiple storage and communication modules, guidelines and frameworks related to CAVs forensics are lacking, and traditional digital forensic techniques are not applied owing to the complex requirements and architecture of CAVs. Below, we categorize the forensic challenges faced by CAVs into two categories:

1) **Technical Challenges:** Every CAV involves a range of devices that can be used as digital evidence to perform forensic investigations. Typical data sources of digital evidence include the following:

(i) Event Data Recorder (Black Box)
(ii) Vehicle Infotainment System
(iii) Electronic Control Units (ECU)
(iv) Key Fobs
(v) Multiple Sensors
(vi) Journey Logs

With this wide range of data sources, complexity and quantity have become issues that make it difficult to gather evidence. Some of these issues include the following:

a) How can we categorize what data to store inside the vehicle, what goes on the cloud, and for how long?
b) Which software tool/framework is suitable for performing data acquisition for a large amount of online and offline data simultaneously without compromising its integrity?
c) Where is the data stored internally? RAM, flash, EPROM, or USB drive.
d) CAVs can capture and analyze diverse types of data on the fly, which may involve different processing protocols. How can such data be handled?

2) **Legal Challenges:** The lack of vehicle forensic guidelines in the automotive industry is concerning. Therefore, there is a need for a paradigm shift in forensic techniques to analyze CAVs data. To ensure admissibility in legal proceedings for vehicle forensics, we need to ensure the fulfillment of data properties, such as confidentiality, integrity, availability, authenticity, non-reputation, and privacy. Some legal issues surrounding CAVs forensics are as follows:

- The reliability and accuracy of forensic evidence have also been proven. Digital data can be captured, therefore, seizing and freezing digital inference can no longer be accomplished by burning the CD-ROM. Failure to freeze the evidence before opening the files invalidates critical evidence.
- CAVs must map their surroundings to understand their environment and work efficiently; However, the mapping of private property can be considered an intrusion. To ensure privacy, guidelines on which data can be captured and stored by CAVs must be clearly defined.
- Another issue is finding relevant evidence from the massive amounts of data. Real legal challenges in terms of limitations imposed by constitutional, statutory, and procedural issues. Many types of personnel are involved in CAVs forensics, including technicians, policymakers, professionals, and insurers.
- Finally, technicians require sound knowledge and special skills to gather digital evidence and have a good understanding of software, hardware, and networks. Therefore, technicians should be provided with intensive training including technical

skills and legal procedures, before becoming involved in CAV forensics.

VI. EXISTING SOLUTIONS

The current state of established solutions for connected autonomous vehicles is volatile and erratic. Most experimental testing is performed behind closed doors; however, for the work that is published and in the public domain, limited insight is shared with those researching or analyzing the situation. In Table 2, we share state-of-the-art solutions for sensor, communication, and actuator attacks based on two categories:

A. EXISTING SOLUTIONS TO CYBERATTACKS

In this section, we analyze existing solutions to cyber security risks and vulnerabilities in CAVs. For a better understanding, we shared insights into traditional, and AI-based technologies as follows:

1) TRADITIONAL SOLUTIONS

These include conventional software programming solutions, in which the solution is built by a human based on sets of manually defined rules. The output was predictable and constant with less room for feedback and self-training. Coding is the primary artifact of traditional solutions, where some input is given to the algorithm along with the logic code, which is finally drummed up into the output. Traditional solutions are rule-based, in which rules are clearly defined and implemented in a programming language regarding how the system should function and behave under certain conditions.

2) AI-BASED SOLUTIONS

Connected Autonomous Vehicles generate massive volumes of data every minute from millions of devices. Machine Learning techniques are based on obtaining devices to make decisions and to act without explicit programming. Machine Learning algorithms enable CAVs to exist because they require sensors to collect data, fuse data, and make decisions. The technique requires analyzing the logs and patterns for decision making, which could further help to warn and even mitigate any risks occurring within the device.

After the logs are collected and stored, machine-learning technology can be used to analyze and detect the data within the logs to determine if there are any abnormal data. As machine learning enhances the detection model, algorithms can be used to detect malware activities and unusual vehicle behaviors. Detection algorithms become even better when combined with data from an Intelligent Transportation System. This complete network is considered a proprietary system that works quite differently from average computer networks, making it easier to predict vehicle movements [131]. Machine learning should be deployed to train sensor data algorithms to promptly detect malicious activities.

B. EXISTING SOLUTIONS TO FORENSIC

The purpose of CAVs forensics is to acquire data and develop a timetable of events to provide courts with accurate information on criminal activity or accidents. Vehicle forensics is an emerging field, and the authors of [132], [133] explored this new branch of forensics by performing forensics on a real testbed. Their work demonstrated that although standardized guidelines on CAV forensics are not yet available, there are several existing branches of forensic and software testing techniques that could play a key role in CAVs after a crash investigation. Below, we discuss four of these:

1) **Digital Forensics:** Digital devices form a large set of connected nodes that share significant similarities with CAVs in forensic investigations. The physical and digital world interaction in emerging devices also leads to further investigation techniques, owing to the increased variety of data storage and exchange mechanisms. The skillset derived from digital device security and forensics is also applicable to CAVs.
2) **Cyber Physical System (CPS) Forensics:** CPSs have multiple computing components including nodes, sensors, actuators, smart devices, and software. These components are connected via wired networks and/or different types of wireless networks to control the physical environment of the system. CAVs are a subset of CPS, therefore, knowledge is directly transferable.
3) **Software Reliability Analysis:** Preemptive approaches to CAV incidents can also be helpful in the assessment of incidents. Reliability analyses of individual and integrated components will also reveal the weaknesses and vulnerabilities of CAVs from various manufacturers. This analysis can be effective in identifying the components on which investigators must focus.
4) **Penetration Testing:** Pen testing is critical for assessing the overall strength and vulnerability of IoT devices to cyber-attack.

VII. OBSERVATION AND DISCUSSION

A critical aspect of any emerging technology is its security standard, which encompasses and covers all forms. Designing technology to ensure preservation is a necessary practice; however, with the emergence of CAVs, this is now a noticeable issue. Although this is not due to a lack of effort for innovation it is the opposite; – the initiative to create fully-functional CAVs presents challenges that obstruct the success of these standards. In this section, we discuss several important challenges in CAVs' security and forensics. The aspects listed here culminate in why cybersecurity is imperative for the future of CAVs. In addition, several research directions were outlined.

A. SECURITY AMONG CUSTOMERS

Many factors influence the psychology of consumers to feel ''unsafe'' with a purchase, such as brand loyalty or reliability; CAVs are no exception to these commonalities. Rather than

TABLE 2. Summary of existing traditional, and AI-based defense solutions in the CAVs.

Attack Type		Traditional Defense Strategies	AI Defense Strategies
Sensor	Spoofing	[66]–[68]	[69], [70]
	Jamming	[71]–[73]	[74], [75]
	Tampering	[76], [77]	[78]
	Adversarial	**N/A**	[45],[79], [80]
	Denial of Service	[81], [82]	[83]–[86]
Communication	Sybil	[87], [88]	[89]–[92]
	Replay	[93], [94]	[95], [96]
	Relay	[97], [98]	[99], [100]
	Remote	[101]	[102],[103]
	Malware	[104]	[105],[106]
	Impersonation	[107]–[109]	[110], [111]
	Data Falsified	[112]–[114]	[19], [115], [116]
	Man in the Middle	[117], [118]	[119]
	Blackhole/Greyhole	[120], [121]	[122] –[124]
Actuator	Sensor Fusion	[62], [125]	[102], [126], [127]
	Piggy Backing	**N/A**	[128]
	Supply Chair	[129]	[130]

deliberating on worthy investments, vehicle owners would want to ensure physical safety. Statistics reveal that 45% of those surveyed in the United States claim that they do not feel secure in autonomous self-driving cars [134]. Incidents such as those involving the Volvo XC90 and Tesla Model X have contributed to shaky early impressions of autonomous vehicles [135]. In the world of commercialism, the mystique of self-driving cars is vague; however, this is before these vehicles are allowed in the hands of consumers. The perception of autonomous vehicles by the general population is reliant on these limited events, and autonomous cars are comparable to niches of other technologies. In addition to cybersecurity, autonomous cars need to prove their safety features through rigorous testing and results that shed a positive light on technology. Self-driving car sensors, artificial intelligence, and machine learning must be performed through simulations and experiments using real vehicles [135]. Therefore, the first step before cybersecurity fortification is to improve the reputation of autonomous vehicles by developing and displaying their safety functionalities.

B. STANDARDIZATION GAP

To ensure the resilience of vehicles against cyber-attacks, they must be tested extensively. As discussed in Section IV, standards related to functional safety, SAE J3061, and ISO 21448 exist; however, none have addressed the issues and regulations when AI-based algorithms are introduced into autonomous driving systems (Figure 8). Standards should include details on (i) establishing trust in AI through transparency, verifiability, explicability, and controllability, (ii) investigating the threats and risks of using AI-based systems, and (iii) investigating approaches to achieving AI system robustness, resiliency, safety, privacy, and accuracy; as these are all crucial pillars for AI deployment in CAVs.

C. 5G VS. DSRC

The security of CAVs relies heavily on the data packets transmitted over the communication network to make informed decisions regarding their speed and maneuvering. Therefore, packet delays and drops in communication networks can negatively affect the occurrence of accidents and fatalities. The debate over 5G and DSRC has been ongoing for the past couple of years, where each technology has proven its capability in one way or the other, and the effectiveness of both still requires testing in real-world scenarios before the deployment of CAVs. As 5G and connected vehicle technologies are still in progress, time will determine how DSRC and 5G will interoperate.

D. DATA STORAGE

Data is the most valuable entity for automotive players, as connectivity makes its way into both vehicles and the environment. By 2023, there are expected to be 37.9 million vehicles on the road, generating 300 petabytes of data annually, with at least five TB of data generated per day. The data were obtained from onboard hardware, which included data from several sensors. Data are stored, transferred, and secured across many endpoints over various delivery networks. The biggest question here is which storage approach should be adopted to manage data. This issue becomes even more tedious as 5G approaches quickly, which requires automakers to search for the best storage choice, considering cost and performance as the principal factors.

E. COMPUTING CHALLENGES

To prevent fatalities, CAVs use multiple sensor inputs to collect enormous amounts of data through visual processing and object detection. However, the challenge lies in the efficient processing and delivery of high volumes of data in communication networks. A delay of even milliseconds can result in fatal collisions on roads. OEMs such as Google, Tesla, and several start-ups, have already started focusing on bridging the gap between vehicle data and computing ecosystems by building solutions that offer low latency and faster decisions [137]. Solutions, including cloud computing and NVIDIA's Drive DGX, have proven enormous potential

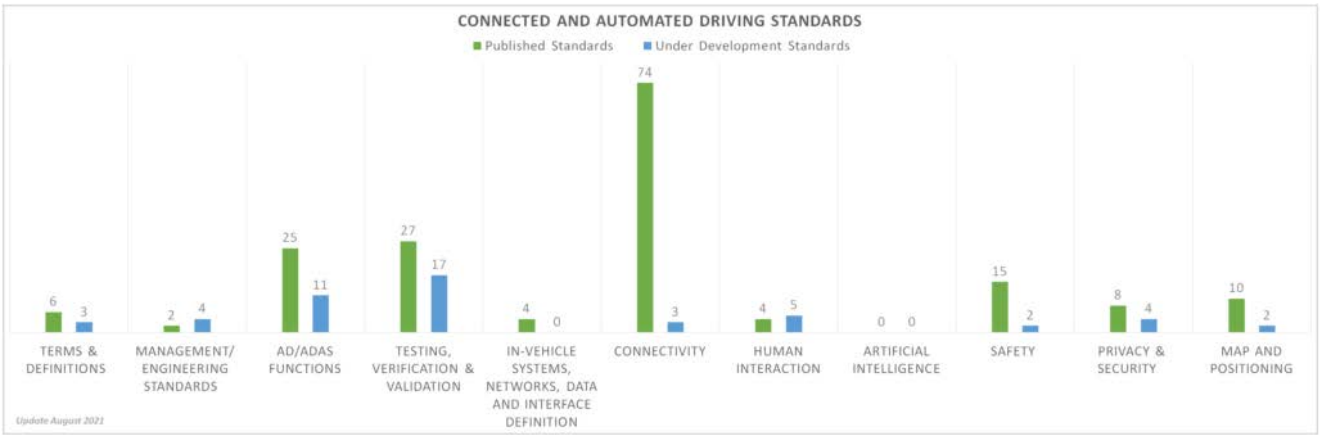

FIGURE 8. Connected autonomous vehicle driving standards [136].

in edge computing; however, much work is still required to enhance the judgment of CAVs in unforeseen situations.

F. SOFTWARE UPDATE MANAGEMENT

As the number of CAVs increases, the amount of data generated and the cost and complexity of collecting data and managing subscriptions also increase. This forces OEMs to pay close attention to the partners with whom they decide to collaborate. Further, the geographical region, chosen communications service providers (CSP), and performance requirements are the dependent variables that directly affect the market. In addition, the costs associated with managing CSP relationships and different vehicle profiles accessing the cellular network, and the costs associated with connectivity and profile management must remain predictable and low [138]. Therefore, OEMs need to address the following questions: (I) If all the data are treated equally and billed to one subscriber, who will pay for it? (ii) Who pays for the software updates?, (iii) Are OEMs willing to pay for the entertainment-based data usage consumed by passengers? [138]

G. SENSOR FUSION CHALLENGES

Sensors are the backbone of CAVs, and allow vehicles to view the road ahead, to the side, and behind. Therefore, developing robust sensors is a key priority for OEMs, and combining sensor data is an essential part of the autonomy puzzle. One significant issue with sensor fusion is the multimodality of the data at the acquisition and data source levels. All sensors have different physical units of measurement, sampling resolutions, and spatial-temporal alignment. In addition, there is huge uncertainty in data sources, including noise related to calibration/quantization errors, precision losses, inconsistent data, and missing values. The industry is actively working on developing more robust, reliable, and safe approaches for data fusion, which considers uncertainty in the fusion algorithm, and data fusion algorithms that work with minimal calibration.

H. SUPPLY CHAIN CHALLENGES

OEMs rely on Tier 1, Tier 2, or chipmakers for the most updated electronic and chip technology solutions. However, this trend has changed over the past decade, when OEMs are now investing more in research on system design, modeling, and simulation. Therefore, instead of relying on suggestions from the supply chain, OEMs are discovering features by themselves that they would need a new vehicle design enabling the change in basic assumptions for OEMs to take the lead. The results generated from the simulation aid OEMs in understanding the highly specific features required for CAVs designs that are further communicated to chipmakers. This new trend is burdening chipmakers to develop customized cost-effective solutions that are scalable and upgradable to meet the needs of OEMs, thereby creating supply chain challenges.

I. POLICY AND LAWS

In the case of an accident, the primary duty of the first responders is to supply safety to the people, and then clean up the road to allow traffic to flow. However, first responders are neither equipped nor ready to forensically investigate accidents or car wrecks that involve CAVs. Even if equipped, data curation from damaged hardware (i) take considerable time, (ii) is not guaranteed to supply complete data owing to damage beyond saving, and (iii) must be performed in an undisturbed environment, which may be impossible on highways at the scene of an accident. Furthermore, a successful investigation involves finding and substantiating the relevant evidence as quickly as possible [139]. While forensic tools are potent weapons in the cyber world they are insufficient to overcome the challenge of the complex data generated by CAVs [139]. It is beyond ordinary human capabilities to examine the amount of data generated by CAVs to promptly perform an investigation. While the collection of digital evidence requires the technical ability and tools necessary to curate information as evidence, forensic investigators must consider and act on legal factors, such as *personal privacy*

issues. CAVs are widely considered computer systems, and therefore, policies involving attacks and investigation of computer systems are directly applicable. However, how these policies and laws are applicable remains unclear as CAVs are Cyber-Physical Systems, and therefore, investigations involving physical and digital elements are bound to create overlaps, issues, and even problems on the scope of authority between law enforcement entities.

VIII. CONCLUSION

CAVs have shown immense potential in reducing traffic accidents, enhancing the quality of life, and promoting safe and efficient transportation systems. However, there are still many challenges in terms of security, privacy, and forensics in the CAV technology. This work offers an in-depth analysis of the existing literature on cyberattacks, defense mechanisms, and forensic perspectives of CAVs. First, we introduce the components of connectivity, autonomy, and intelligent transportation systems, followed by the existing security and forensic standards/protocols built specifically for CAVs. The authors then distinguished potential cyber-attacks on CAVs based on the sensor, communication, and actuator networks. Next, we surveyed the existing cyberattack defense strategies based on traditional and artificial intelligence techniques. Finally, we present the open challenges and issues in current CAVs security and forensics.

We hope that this study will help researchers in this field by providing an overview of the current state of the ITS and CAVs development. This study also assists in the research and development of cybersecurity defense solutions for ITS networks.

ACKNOWLEDGMENT

The authors would like to thank Dr. Gokhan Kul, Assistant Professor, at the University of Massachusetts, Dartmouth, for his valuable time and assistance with CAVs forensics.

REFERENCES

[1] J. M. Coren. (2018). *All the Places Self-Driving Cars Are Being Tested Around the World*. Accessed: Feb. 19, 2022. [Online]. Available: https://qz.com/1488576/self-driving-car-tests-around-the-world/

[2] AutoPilot Review. (2021). *Cars With Autopilot in 2021*. Accessed: Jun. 19, 2021. [Online]. Available: https: www.autopilot review.com/cars-with-autopilot-self-driving

[3] *Taxonomy and Definitions for Terms Related to Driving Automation Systems for on-Road Motor Vehicles*, Standard J3016_202104, Society of Automotive Engineers—SAE International, 2018. [Online]. Available: https://www.sae.org/standards/content/j3016_202104/

[4] 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.

[5] A. Krietz, "Tesla driver, passenger killed after crashing into back of semi-truck off I-75," WTSP News, Tech. Rep., 10, Accessed: Jul. 15, 2022. [Online]. Available: https://www.wtsp.com/article/news/regional/florida/deadly-tesla-crash-gainesville-florida-nhtsa-investigation/67-20e37a6f-dab1-4b23-8090-daeba419f787

[6] D. Wakabayashi. *Self-Driving Uber Car Kills Pedestrian in Arizona Where Robots Room*. Accessed: Sep. 30, 2019. [Online]. Available: https://www.nytimes.com/2018/03/19/technology/uber-driverlessfatality.html

[7] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6240–6259, Jul. 2022.

[8] 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.

[9] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Comput. Secur.*, vol. 103, Apr. 2021, Art. no. 102150.

[10] 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*.

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

[12] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors J.*, vol. 20, no. 22, pp. 13752–13767, Nov. 2020.

[13] A. D. Kumar, K. N. R. Chebrolu, and K. P. Soman, "A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities," 2018, *arXiv:1810.04144*.

[14] *What's Happening With Automated Vehicles?*. Accessed: Feb. 21, 2022. [Online]. Available: https://www.selfdrivingcars360.com/whats-happening-with-automatedvehicles/

[15] B. S. Jahromi, T. Tulabandhula, and S. Cetin, "Real-time hybrid multi-sensor fusion framework for perception in autonomous vehicles," *Sensors*, vol. 19, no. 20, p. 4357, Oct. 2019.

[16] D. J. Yeong, G. Velasco-Hernandez, J. Barry, and J. Walsh, "Sensor and sensor fusion technology in autonomous vehicles: A review," *Sensors*, vol. 21, no. 6, p. 2140, Mar. 2021.

[17] *Why Optical Phased Array is the Future of LiDAR for Autonomous Vehicles*. Accessed: Jun. 21, 2022. [Online]. Available: https://lidarmag.com/2021/08/18/why-optical-phased-array-isthe-future-of-lidar-for-autonomous-vehicles/

[18] G. M. Smith. (2021). *What is ADAS (Advanced Driver Assistance Systems)?*. Accessed: Jul. 25, 2022. [Online]. Available: https://dewesoft.com/daq/what-is-adas

[19] P. Sharma, H. Liu, H. Wang, and S. Zhang, "Securing wireless communications of connected vehicles with artificial intelligence," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Apr. 2017, pp. 1–7.

[20] *SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary*, DSRC Committee, SAE Standard 2735-201, 2015.

[21] *On-Board System Requirements for V2V Safety Communications*, Standard J2945/1_202004, Society of Automotive Engineers—SAE International, 2020. [Online]. Available: https://www.sae.org/standards/content/j2945/1_202004/

[22] *What is IEEE 802.11p?*. Accessed: Mar. 21, 2022. [Online]. Available: https://www.everythingrf.com/community/whatis-ieee-802-11p

[23] *IEEE 1609—Family of Standards for Wireless Access in Vehicular Environments (WAVE)*. Accessed: Jul. 21, 2022. [Online]. Available: https://www.standards.its.dot.gov/Factsheets/Factsheet/80

[24] J. Guerrero-Ibáñez, S. Zeadally, and J. Contreras-Castillo, "Sensor technologies for intelligent transportation systems," *Sensors*, vol. 18, no. 4, p. 1212, Apr. 2018.

[25] J. Zhao, H. Xu, H. Liu, J. Wu, Y. Zheng, and D. Wu, "Detection and tracking of pedestrians and vehicles using roadside LiDAR sensors," *Transp. Res. C, Emerg. Technol.*, vol. 100, pp. 68–87, Mar. 2019.

[26] B. Barbagli, G. Manes, R. Facchini, and A. Manes, "Acoustic sensor network for vehicle traffic monitoring," in *Proc. 1st Int. Conf. Adv. Veh. Syst., Technol. Appl.*, 2012, pp. 24–29.

[27] Tim Weisenberger. *SAE and ISO Publish Joint Automotive Cybersecurity Standard*. Accessed: Jan. 5, 2022. [Online]. Available: https://sae.org/news/2021/09/sae-and-iso-publish-jointautomotive-cybersecurity-standard

[28] Beyond Security. (2021). *A Beginner's Guide to the ISO/SAE 21434 Cybersecurity Standard for Road Vehicles*. Accessed: Feb. 10, 2022. [Online]. Available: https://blog.beyondsecurity.com/iso-sae-21434-standard-road-vehicles/

[29] *WP.29 Cybersecurity Vehicle Regulation Compliance*. Accessed: Mar. 12, 2022. [Online]. Available: https://blackberry.qnx.com/en/ultimate-guides/wp-29-vehiclecybersecurity

[30] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner, "Using SAE J3061 for automotive security requirement engineering," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.* Cham, Switzerland: Springer, 2016, pp. 157–170.
[31] I. C. Schlenoff and V. Nguyen, "Standards and performance metrics for on-road autonomous vehicles," in *Proc. NIST Workshop*, Mar. 2022. [Online]. Available: https://www.nist.gov/news-events/events/2022/03/standards-and-performance-metrics-road-autonomous-vehicles
[32] S. Alharbi, J. Weber-Jahnke, and I. Traore, "The proactive and reactive digital forensics investigation process: A systematic literature review," in *Proc. Int. Conf. Inf. Secur. Assurance*. Berlin, Germany: Springer, 2011, pp. 87–100.
[33] R. S. C. Ieong, "FORZA—Digital forensics investigation framework that incorporate legal issues," *Digit. Invest.*, vol. 3, pp. 29–36, Sep. 2006.
[34] K. K. G. Buquerin, "Analysis of digital forensics capabilities on state-of-the-art vehicles," Ph.D. thesis, Dept. Comput. Sci., Technische Hochschule Ingolstadt, Ingolstadt, Germany, 2019.
[35] P. Sharma, U. Siddanagaiah, and G. Kul, "Towards an AI-based after-collision forensic analysis protocol for autonomous vehicles," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2020, pp. 240–243.
[36] J. P. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," Black Hat Eur., Amsterdam, The Netherlands, 2015, p. 995, vol. 11, no. 2015.
[37] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *Proc. Int. Conf. Cryptograph. Hardw. Embedded Syst.* Cham, Switzerland: Springer, 2017, pp. 445–467.
[38] G.-H. Lee, J. Jo, and C. H. Park, "Jamming prediction for radar signals using machine learning methods," *Secur. Commun. Netw.*, vol. 2020, pp. 1–9, Jan. 2020.
[39] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, no. 8, p. 109, Aug. 2016.
[40] B. S. Lim, S. L. Keoh, and V. L. L. Thing, "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Feb. 2018, pp. 231–236.
[41] H. Shin, Y. Son, Y. Park, Y. Kwon, and Y. Kim, "Sampling race: Bypassing timing-based analog active sensor spoofing detection on analog-digital systems," in *Proc. 10th USENIX Workshop Offensive Technol. (WOOT)*, 2016, pp. 1–11.
[42] 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.
[43] J. Li, F. Schmidt, and Z. Kolter, "Adversarial camera stickers: A physical camera-based attack on deep learning systems," in *Proc. Int. Conf. Mach. Learn.*, 2019, pp. 3896–3904.
[44] C. DiPalma, N. Wang, T. Sato, and Q. A. Chen, "Security of camera-based perception for autonomous driving under adversarial attack," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2021, p. 243.
[45] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust LiDAR-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures," in *Proc. 29th Secur. Symp.*, Aug. 2020, pp. 877–894.
[46] A. Modas, R. Sanchez-Matilla, P. Frossard, and A. Cavallaro, "Toward robust sensing for autonomous vehicles: An adversarial perspective," *IEEE Signal Process. Mag.*, vol. 37, no. 4, pp. 14–23, Jul. 2020.
[47] B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," M.S. thesis, Dept. Elect. Eng., Math. Comput. Sci. (EEMCS), Univ. Twente, Enschede, The Netherlands, 2015.
[48] M. Soni and A. Jain, "Secure communication and implementation technique for Sybil attack in vehicular ad-hoc networks," in *Proc. 2nd Int. Conf. Comput. Methodologies Commun. (ICCMC)*, Feb. 2018, pp. 539–543.
[49] J. R. Douceur, "The Sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.
[50] *Honda Downplays Vulnerability Allowing Hackers to Lock, Unlock and Start Civics*. Accessed: Jul. 19, 2022. [Online]. Available: https://malware.news/t/honda-downplays-vulnerability-allowinghackers- to-lock-unlock-and-start-civics/58692
[51] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, 2011, pp. 1–16.
[52] *Hackers Remotely Kill a Jeep on the Highway-With me in it*. Accessed: Jun. 8, 2022. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[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.*, 2016, pp. 1–17.
[54] J. Markoff. (2011). *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*. Accessed: Jun. 19, 2022. [Online]. Available: https://www.nytimes.com/2011/03/10/business/10hack.html?_r=0
[55] C. Miller and C. Valasek. (2015). Accessed: Jun. 1. 2022. [Online]. Available: https://www.nytimes.com/2011/03/10/business/10hack.html?
[56] I. A. Sumra, H. B. Hasbullah, and J.-L. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey," in *Vehicular Ad-hoc Networks for Smart Cities*. Singapore: Springer, 2015, pp. 51–61.
[57] M. R. Ghori, K. Z. Zamli, N. Quosthoni, M. Hisyam, and A. Montaser, "Vehicular ad-hoc network (VANET)," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, May 2018, pp. 1–6.
[58] R. Mishra, A. Singh, and R. Kumar, "VANET security: Issues, challenges and solutions," in *Proc. Int. Conf. Electr., Electron., Optim. Techn. (ICEEOT)*, Mar. 2016, pp. 1050–1055.
[59] M. A. H. A. Junaid, A. Syed, M. N. M. Warip, K. N. 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, 2018, p. 06038.
[60] F. Ahmad, A. Adnane, V. N. Franqueira, F. Kurugollu, and L. Liu, "Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies," *Sensors*, vol. 18, no. 11, p. 4040, 2018.
[61] V. Bibhu, K. Roshan, K. B. Singh, and D. K. Singh, "Performance analysis of black hole attack in VANET," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 11, pp. 47–54, Oct. 2012.
[62] Y. Cao, N. Wang, C. Xiao, D. Yang, J. Fang, R. Yang, Q. A. Chen, M. Liu, and B. Li, "Invisible for both camera and LiDAR: Security of multi-sensor fusion based perception in autonomous driving under physical-world attacks," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 176–194.
[63] L. Li, D. Li, T. F. Bissyandé, J. Klein, Y. L. Traon, D. Lo, and L. Cavallaro, "Understanding Android app piggybacking: A systematic study of malicious code grafting," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1269–1284, Jun. 2017.
[64] M. Ohm, H. Plate, A. Sykosch, and M. Meier, "Backstabber's knife collection: A review of open source software supply chain attacks," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*, C. Maurice, L. Bilge, G. Stringhini, and N. Neves, Eds. Cham, Switzerland: Springer, 2020, pp. 23–43.
[65] S. K. Khan, N. Shiwakoti, P. Stasinopoulos, and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," *Accident Anal. Prevention*, vol. 148, Dec. 2020, Art. no. 105837.
[66] 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.
[67] S. Bittl, A. A. Gonzalez, M. Myrtus, H. Beckmann, S. Sailer, and B. Eissfeller, "Emerging attacks on VANET security based on GPS time spoofing," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Sep. 2015, pp. 344–352.
[68] D. Kosmanos, A. Pappas, L. Maglaras, S. Moschoyiannis, F. J. Aparicio-Navarro, A. Argyriou, and H. Janicke, "A novel intrusion detection system against spoofing attacks in connected electric vehicles," *Array*, vol. 5, Mar. 2020, Art. no. 100013.
[69] S. Semanjski, I. Semanjski, W. D. Wilde, and A. Muls, "Use of supervised machine learning for GNSS signal spoofing detection with validation on real-world meaconing and spoofing data—Part I," *Sensors*, vol. 20, no. 4, p. 1171, 2020.
[70] A. Shafique, A. Mehmood, and M. Elhadef, "Detecting signal spoofing attack in UAVs using machine learning models," *IEEE Access*, vol. 9, pp. 93803–93815, 2021.
[71] A. Mpitziopoulos, D. Gavalas, G. Pantziou, and C. Konstantopoulos, "Defending wireless sensor networks from jamming attacks," in *Proc. IEEE 18th Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2007, pp. 1–5.
[72] O. Osanaiye, S. A. Alfa, and G. P. Hancke, "A statistical approach to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 18, no. 6, p. 1691, May 2018.
[73] M. Adil, M. A. Almaiah, A. A. Omar, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, p. 2311, Jan. 2020.

[74] L. Jia, Y. Xu, Y. Sun, S. Feng, and A. Anpalagan, "Stackelberg game approaches for anti-jamming defence in wireless networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 120–128, 2018.

[75] D. Karagiannis and A. Argyriou, "Jamming attack detection in a pair of RF communicating vehicles using unsupervised machine learning," *Veh. Commun.*, vol. 13, pp. 56–63, Jul. 2018.

[76] F. R. Salmasi, "A self-healing induction motor drive with model free sensor tampering and sensor fault detection, isolation, and compensation," *IEEE Trans. Ind. Electron.*, vol. 64, no. 8, pp. 6105–6115, Aug. 2017.

[77] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1319–1330, Jul. 2013.

[78] A. K. Pathak, S. Saguna, K. Mitra, and C. Ahlund, "Anomaly detection using machine learning to discover sensor tampering in IoT systems," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6.

[79] Z. Tang, M. Kuijper, M. S. Chong, I. Mareels, and C. Leckie, "Linear system security—Detection and correction of adversarial sensor attacks in the noise-free case," *Automatica*, vol. 101, pp. 53–59, Mar. 2019.

[80] S. Kokalj-Filipovic, R. Miller, N. Chang, and C. L. Lau, "Mitigation of adversarial examples in RF deep classifiers utilizing AutoEncoder pre-training," in *Proc. Int. Conf. Mil. Commun. Inf. Syst. (ICMCIS)*, May 2019, pp. 1–6.

[81] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5015–5029, Dec. 2018.

[82] S. Lee, W. Choi, and D. H. Lee, "Securing ultrasonic sensors against signal injection attacks based on a mathematical model," *IEEE Access*, vol. 7, pp. 107716–107729, 2019.

[83] Y. Deng, T. Zhang, G. Lou, X. Zheng, J. Jin, and Q.-L. Han, "Deep learning-based autonomous driving systems: A survey of attacks and defenses," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 7897–7912, Dec. 2021.

[84] T. R. Andel, J. T. McDonald, T. Johnsten, and T. Thomas, "Detection and defense of cyberattacks on the machine learning control of robotic systems," *J. Defense Model. Simul.*, vol. 2021, Nov. 2021, Art. no. 15485129211043874.

[85] F. S. D. L. Filho, F. A. F. Silveira, A. de Medeiros Brito, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Oct. 2019.

[86] 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.

[87] C. Pu, "Sybil attack in RPL-based Internet of Things: Analysis and defenses," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4937–4949, Jun. 2020.

[88] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," *Secur. Commun. Netw.*, vol. 6, no. 4, pp. 523–538, 2013.

[89] A. Alharbi, M. Zohdy, D. Debnath, R. Olawoyin, and G. Corser, "Sybil attacks and defenses in Internet of Things and mobile social networks," *Int. J. Comput. Sci. Issues*, vol. 15, no. 6, pp. 36–41, 2018.

[90] M. Mounica, R. Vijayasaraswathi, and R. Vasavi, "Detecting Sybil attack in wireless sensor networks using machine learning algorithms," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 1042, no. 1, Jan. 2021, Art. no. 012029.

[91] M. Al-Qurishi, M. Al-Rakhami, A. Alamri, M. Alrubaian, S. M. M. Rahman, and M. S. Hossain, "Sybil defense techniques in online social networks: A survey," *IEEE Access*, vol. 5, pp. 1200–1219, 2017.

[92] J. J. Q. Yu, "Sybil attack identification for crowdsourced navigation: A self-supervised deep learning approach," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4622–4634, Jul. 2021.

[93] M. A. Al-shareeda, M. Anbar, I. H. Hasbullah, S. Manickam, N. Abdullah, and M. M. Hamdi, "Review of prevention schemes for replay attack in vehicular ad hoc networks (VANETs)," in *Proc. IEEE 3rd Int. Conf. Inf. Commun. Signal Process. (ICICSP)*, Sep. 2020, pp. 394–398.

[94] F. Miao, M. Pajic, and G. J. Pappas, "Stochastic game approach for replay attack detection," in *Proc. 52nd IEEE Conf. Decis. Control*, Dec. 2013, pp. 1854–1859.

[95] G. Lavrentyeva, S. Novoselov, E. Malykh, A. Kozlov, O. Kudashev, and V. Shchemelinin, "Audio replay attack detection with deep learning frameworks," in *Proc. Interspeech*, Aug. 2017, pp. 82–86.

[96] P. Nagarsheth, E. Khoury, K. Patil, and M. Garland, "Replay attack detection using DNN for channel discrimination," in *Proc. Interspeech*, 2017, pp. 97–101.

[97] J. K. Tugnait, "Detection of active eavesdropping attack by spoofing relay in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 460–463, Oct. 2016.

[98] A. Levi, E. Çetintaş, M. Aydos, Ç. K. Koç, and M. U. Çaglayan, "Relay attacks on Bluetooth authentication and solutions," in *Proc. Int. Symp. Comput. Inf. Sci.* Berlin, Germany: Springer, 2004, pp. 278–288.

[99] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei, "Secure passive keyless entry and start system using machine learning," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Cham, Switzerland: Springer, 2018, pp. 304–313.

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

[101] I. Ngomane, M. Velempini, and S. V. Dlamini, "The design of a defence mechanism to mitigate the spectrum sensing data falsification attack in cognitive radio ad hoc networks," in *Proc. Int. Conf. Adv. Comput. Commun. Eng. (ICACCE)*, Nov. 2016, pp. 237–241.

[102] J. Guan, X. Zheng, C. Wang, Y. Zhou, and A. Jolfa, "Robust sensor fusion algorithms against voice command attacks in autonomous vehicles," 2021, *arXiv:2104.09872*.

[103] S. Lal, S. U. Rehman, J. H. Shah, T. Meraj, H. T. Rauf, R. Damaševičius, M. A. Mohammed, and K. H. Abdulkareem, "Adversarial attack and defence through adversarial training and feature fusion for diabetic retinopathy recognition," *Sensors*, vol. 21, no. 11, p. 3922, Jun. 2021.

[104] M. H. 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.

[105] D. Arivudainambi, V. K. Ka, and P. Visu, "Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance," *Comput. Commun.*, vol. 147, pp. 50–57, Nov. 2019.

[106] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: A deep learning based intrusion detection method in VANET," in *Proc. IEEE 5th Int. Conf. Big Data Secur. Cloud (BigDataSecurity) Int. Conf. High Perform. Smart Comput., (HPSC) IEEE Int. Conf. Intell. Data Secur. (IDS)*, May 2019, pp. 288–293.

[107] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication," *IEEE Syst. J.*, vol. 14, no. 1, pp. 520–529, Mar. 2020.

[108] J. Li, Y. Ji, K.-K. R. Choo, and D. Hogrefe, "CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10332–10343, Aug. 2019.

[109] A. K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5535–5548, Mar. 2020.

[110] S. J. Lee, P. D. Yoo, A. T. Asyhari, Y. Jhi, L. Chermak, C. Y. Yeun, and K. Taha, "IMPACT: Impersonation attack detection via edge computing using deep autoencoder and feature abstraction," *IEEE Access*, vol. 8, pp. 65520–65529, 2020.

[111] S. Chen, K. Ren, S. Piao, C. Wang, Q. Wang, J. Weng, L. Su, and A. Mohaisen, "You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 183–195.

[112] Q. Wang, W. Tai, Y. Tang, and M. Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 2, pp. 101–107, Jun. 2019.

[113] H. T. Reda, A. Anwar, A. N. Mahmood, and Z. Tari, "A taxonomy of cyber defence strategies against false data attacks in smart grid," 2021, *arXiv:2103.16085*.

[114] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: Attack models, targets, and impacts," *Renew. Sustain. Energy Rev.*, vol. 163, Jul. 2022, Art. no. 112423.

[115] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for Internet of Vehicles," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4991–4999, Mar. 2021.
[116] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proc. 17th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Dec. 2018, pp. 564–571.
[117] R. Anderson, "The man-in-the-middle defence," in *Proc. Int. Workshop Secur. Protocols*. Berlin, Germany: Springer, 2006, pp. 157–163.
[118] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—A review," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA)*, Sep. 2017, pp. 1–6.
[119] A. Sebbar, K. Zkik, Y. Baddi, M. Boulmalf, and M. D. E.-C.-E. Kettani, "MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 12, pp. 5875–5894, Dec. 2020.
[120] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks," *Austral. J. Telecommun. Digit. Economy*, vol. 5, no. 1, pp. 50–69, 2017.
[121] J. Jiang, Y. Liu, and B. Dezfouli, "A root-based defense mechanism against RPL blackhole attacks in Internet of Things networks," in *Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC)*, Nov. 2018, pp. 1194–1199.
[122] P. K. Singh, R. R. Gupta, S. K. Nandi, and S. Nandi, "Machine learning based approach to detect wormhole attack in VANETs," in *Proc. Workshops Int. Conf. Adv. Inf. Netw. Appl.* Cham, Switzerland: Springer, 2019, pp. 651–661.
[123] N. Lurski and M. Younis, "Application and mitigation of the evasion attack against a deep learning based IDS for IoT," in *Proc. Int. Conf. Mach. Learn. Netw.* Cham, Switzerland: Springer, 2021, pp. 85–97.
[124] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S. S. Choudhary, V. D. A. Kumar, B. K. Panigrahi, and K. C. Veluvolu, "Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm," *Microprocessors Microsyst.*, vol. 80, Feb. 2021, Art. no. 103352.
[125] S. Schreiber-Ehle and W. Koch, "The JDL model of data fusion applied to cyber-defence—A review paper," in *Proc. Workshop Sensor Data Fusion, Trends, Solutions, Appl. (SDF)*, Sep. 2012, pp. 116–119.
[126] T. Meng, X. Jing, Z. Yan, and W. Pedrycz, "A survey on machine learning for data fusion," *Inf. Fusion*, vol. 57, pp. 115–129, Jan. 2020.
[127] J. Tu, H. Li, X. Yan, M. Ren, Y. Chen, M. Liang, E. Bitar, E. Yumer, and R. Urtasun, "Exploring adversarial robustness of multi-sensor perception systems in self driving," 2021, *arXiv:2101.06784*.
[128] M. Fan, J. Liu, W. Wang, H. Li, Z. Tian, and T. Liu, "DAPASA: Detecting Android piggybacked apps through sensitive subgraph analysis," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1772–1785, Aug. 2017.
[129] J. A. Reuben and N. Ware, "Approach to handling cyber security risks in supply chain of defence sector," *Ind. Eng. J.*, vol. 12, no. 7, pp. 1–12, Jul. 2019.
[130] I. A. Khan, D. N. Moustafa, D. Pi, Y. Hussain, and N. A. Khan, "DFF-SC4N: A deep federated defence framework for protecting supply chain 4.0 networks," *IEEE Trans. Ind. Informat.*, early access, Sep. 1, 2021, doi: 10.1109/TII.2021.3108811.
[131] H. Liu, S. Zhang, P. Zhang, X. Zhou, X. Shao, G. Pu, and Y. Zhang, "Blockchain and federated learning for collaborative intrusion detection in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6073–6084, Jun. 2021.
[132] N.-A. Le-Khac, D. Jacobs, J. Nijhoff, K. Bertens, and K.-K.-R. Choo, "Smart vehicle forensics: Challenges and case study," *Future Gener. Comput. Syst.*, vol. 109, pp. 500–510, Aug. 2020.
[133] K. Strandberg, N. Nowdehi, and T. Olovsson, "A systematic literature review on automotive digital forensics: Challenges, technical solutions and data collection," *IEEE Trans. Intell. Vehicles*, early access, Jul. 4, 2022, doi: 10.1109/TIV.2022.3188340.
[134] M. A. L. Rainie, C. Funk, and A. Tyson. (2022). *Americans Cautious About the Deployment of Driverless Cars*. Accessed: Jul. 10, 2022. [Online]. Available: https://www.pewresearch.org/internet/2022/03/17/americans-cautiousabout-the-deployment-of-driverless-cars/
[135] *Challenges in the Automotive Industry on the Road to Autonomous Driving*. Accessed: Mar. 12, 2021. [Online]. Available: https://intellias.com/challenges-automotive-industryface-autonomous-driving/
[136] *2021 Gaps and Recommendations*. Accessed: Feb. 21, 2022. [Online]. Available: https://rb.gy/bvqm58/
[137] G. Mathew. (2021). *Edge Computing: Tech's Next Trillion-Dollar Opportunity*. Accessed: Jun. 21, 2022. [Online]. Available: https://devops.com/edge-computing-techs-next-trillion-dollaropportunity/
[138] K. Okamoto. (2021). *The 5 Top Connected Car Challenges Faced by Automotive OEMs*. Accessed: Oct. 27, 2021. [Online]. Available: https://www.ericsson.com/en/blog/2021/9/the-5-top-connectedcar-challenges-faced-by-automotive-oems
[139] H. Behl. (2021). *AI Pivotal for Forensic Investigative Teams to Handle Crushing Data Volumes*. Accessed: Mar. 14, 2022. [Online]. Available: https://www.securitymagazine.com/articles/96052- ai-pivotal-for-forensic-investigative-teams-to-handle-crushing-datavolumes

PRINKLE SHARMA received the B.S. degree in information technology from Punjab Technical University, Punjab, India, in 2012, and the M.S. degree in computer and information science and the Ph.D. degree in electrical and computer engineering specializing in cybersecurity networks and artificial intelligence from the University of Massachusetts at Dartmouth (UMass Dartmouth), Dartmouth, MA, USA, in 2016 and 2020, respectively.

From 2015 to 2020, she worked as a Research Assistant with the Internet of Things Laboratory, UMass Dartmouth. Since 2015, she has been working on securing wireless communications in autonomous vehicles by applying artificial intelligence. Since 2020, she has been an Assistant Professor with the Information Security and Digital Forensics Department, University at Albany-State University of New York. She has conducted extensive research in detecting security vulnerabilities in automotive systems. Her work on connected vehicle safety was featured in IEEE Xplore Innovation Spotlight, in 2018. Her research interests include network security, artificial intelligence, human–computer interaction, and machine learning.

JAMES GILLANDERS graduated from the Bayport-Blue Point High School, Bayport, NY, USA, in 2020. He is currently a Junior Researcher at the University at Albany-State University of New York, majoring in informatics with a concentration in software development. Since 2022, he has been working as a Researcher with Dr. Prinkle Sharma on cyber-physical systems security and privacy. His research interests include cyber and information security, sensor networks, and artificial intelligence.