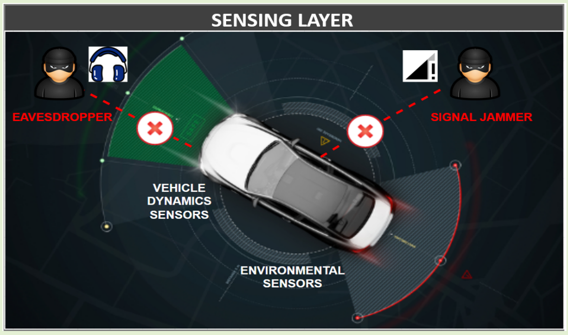
Cybersecurity Attacks in Vehicular Sensors

Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj,
Siby Jose Plathottam, and Prakash Ranganathan, *Senior Member, IEEE*

***Abstract*—Today's modern vehicles contain anywhere from sixty to one-hundred sensors and exhibit the characteristics of Cyber-Physical-Systems (CPS). There is a high degree of coupling, cohesiveness, and interactions among vehicle's CPS components (e.g., sensors, devices, systems, systems-of-systems) across sensing, communication, and control layers. Cyber-attacks in the sensing or communication layers can compromise the security of the control layer. This paper provides a detailed review of potential cyber threats related to the sensing layer. Notably, the focus is mainly towards two categories of sensors: vehicle dynamics sensors (e.g., Tire Pressure Monitoring Systems (TPMS), magnetic encoders, and inertial sensors) and environment sensors (e.g., Light Detection and Ranging (LiDAR), ultrasonic, camera, Radio Detection and Ranging (Radar) systems, and Global Positioning System (GPS) units). The paper also offers perspectives through existing countermeasures from literature and stresses the need for data-driven cybersecurity solutions.**



***Index Terms*—Cyber-attacks, environment sensors, sensing layer, vehicle dynamics sensors.**

I. Introduction

WE ARE rapidly approaching an age in which both partially and fully-autonomous vehicles will emerge on roadway systems. The National Highway Traffic Safety Administration (NHTSA) has set forth a vision that eventually leads to deploying fully autonomous, self-driving cars sometime after the year 2025 [1]. In the meantime, the NHTSA is encouraging the development of partially automated vehicular functions, such as lane-keeping assist, adaptive cruise control, and self-parking.

Auto and technology Original Equipment Manufacturers (OEMs) such as Waymo [2], Tesla [3], GM Cruise [4], and Aptiv [5] have already begun to use vehicular sensors to enable both fully autonomous and semi-autonomous vehicular functions and test those functions on active roads [6]. A survey by Society of Automotive Engineers (SAE) International details the cybersecurity risks in autonomous vehicles [7]. To safely deploy autonomous vehicles with SAE Level 5 autonomous capability [8], it is necessary to analyze the cybersecurity aspects in the decision-making pipeline.

Autonomous vehicles perceive the world primarily through advanced vehicular sensors. These sensors monitor roadways, recognize road signs, identify potential collision threats, and accurately estimate the distance between a vehicle and nearby objects. Human drivers can draw upon experience to make correct judgments even if their perceptions (e.g., vision) are prevented (e.g., rain) or misleading (e.g., wrong hand signals). State-of-the-art decision-making algorithms used in autonomous vehicles can deal with a certain degree of corrupted sensory input; they are not at a stage where they can match human judgment. Hence, vehicular sensors present an opportunity for a malicious actor to create maximum impact with minimal effort. As vehicle manufacturers work to enhance the ability of vehicular sensors to identify threats and react on time, they become increasingly aware that hackers can deceive vehicular sensors into causing chaos on roadways [9].

Incidents of multiple attack types have been reported during testing of unmanned aerial systems and locomotive robots [10]. However, data on autonomous vehicle sensor attacks are sparse since any detected threat is usually fixed by the vehicle's OEM immediately by patching the vehicle software through Over-The-Air (OTA) updates or recalls. There have been few instances of grey/white hat hackers

Manuscript received May 29, 2020; revised June 16, 2020; accepted June 18, 2020. Date of publication June 22, 2020; date of current version October 16, 2020. The associate editor coordinating the review of this article and approving it for publication was Prof. Subhas C. Mukhopadhyay. *(Corresponding author: Niroop Sugunaraj.)*

Zeinab El-Rewini and Prakash Ranganathan are with the Data, Energy, Cyber and Systems (DECS) Laboratory, University of North Dakota (UND), Grand Forks, ND 58201 USA (e-mail: zeinabrewini@gmail.com; prakash.ranganathan@und.edu).

Karthikeyan Sadatsharan is with Honda Research and Development (R&D) Americas, Raymond, OH 43067 USA (e-mail: karthikeyans068@gmail.com).

Niroop Sugunaraj is with the College of Engineering and Mines (CEM), University of North Dakota (UND), Grand Forks, ND 58201 USA (e-mail: niroop.sugunaraj@und.edu).

Daisy Flora Selvaraj is with the Energy and Environmental Research Centre (EERC), University of North Dakota (UND), Grand Forks, ND 58201 USA (e-mail: daisy.selvaraj@und.edu).

Siby Jose Plathottam is with the Energy Systems division of Argonne National Laboratory, Lemont, IL 60439 USA (e-mail: sibyjackgrove@gmail.com).

Digital Object Identifier 10.1109/JSEN.2020.3004275

identifying cybersecurity threats present in advanced driver assistance features that are available in passenger cars. For example, researchers at Keen Security Labs in China demonstrated a couple of exploits through a camera system in a Tesla Model S [11]. There have also been instances of researchers identifying exploits in perception algorithms used in autonomous vehicles. For example, researchers at the University of Michigan have discovered that they can alter road signs to deceive the object detection algorithms that receive input from camera sensors [12]. After the researchers placed stickers on stop signs, camera sensors passed images of the signs to object detection algorithms that subsequently misidentified the stop signs as speed limit signs. If an attacker used the sticker to target an autonomous vehicle approaching an intersection with a stop sign, the vehicle would not be able to recognize the sign until it was a few feet away. The vehicle would not be able to halt in time, thus potentially causing a collision. Similarly, other vehicular sensors, such as radar sensors or ultrasonic sonars, can be deceived to believe that close objects are further away or non-existent objects are near the vehicle [13], [14].

Vehicular sensors are not the only points of weakness within the vehicular ecosystem. Attackers can exploit connected and automated vehicles by hacking roadside infrastructure and stealing ride-hailing user data stored on the cloud. OTA updates make it conducive for automakers to apply software updates and bug fixes remotely. However, this can lead to security issues as a simple faulty patch can lead to malfunctioning and confusion in the system [15], [16]. Since these updates are remotely sent and initiated, the chances of exploitation are high if the security posture of such updates is not well-implemented [17]. The authors in [18] suggest the use of Physically Unclonable Functions (PUFs) with gateway Electronic Control Units (ECUs) to securely decrypt the OTA update sent by the Original Equipment Manufacturers (OEMs). The supply chain, which is an integral part of every vehicular assembly, must also be secured. Since there are multiple third-party suppliers and manufacturers working on each portion of a vehicle, a hack targeted towards any of these OEMs could lead to malfunction. One way to avoid such malfunction for OEMs is to establish cybersecurity requirements for products manufactured by third parties. For instance, OEMs can work closely with third-party manufacturers to identify possible weaknesses in the required components' architecture before mass production.

Regardless, there is an imminent need for a security standard for OTA updates [7]. Though a vehicle's protocol standards (e.g., criteria for the Controller Area Network (CAN) communication bus, for example) restrict any such updates while the vehicle is operational, the authors in [19] experimentally verified that reflashing (or software upgrading) a vehicle's Electronic Control Unit (ECU) can happen while the vehicle was at speed, suggesting a flaw in the standards.

A. Three-Tier Framework for Automotive Systems

Automotive security threats can be classified through the three-tier hierarchical system shown in Fig. 1. Also known as the AutoVSCC (Autonomous Vehicular Sensing Communication and Control) framework [20], the sensing layer is the first layer of the hierarchy and is comprised of vehicular sensors. Threats to the sensing layer include jamming the Global Positioning System (GPS), eavesdropping on communications within Tire Pressure Monitoring Systems (TPMSs), and deceiving ultrasonic sensors so that they perceive non-existent objects. Threats to the sensing layer can propagate upward to the communication layer through the physical-datalink interface to transmute the analog data from the sensors to digital information that can be used for inter-vehicle and intra-vehicular communications. Cybersecurity threats at the communication layer include sending wrong messages intra-vehicle (within a vehicle's communications buses), gaining control of vehicle functionality through infotainment and telematics systems, and eavesdropping on messages sent between vehicles. Threats at both sensing and communication layers can adversely influence the functionality of the control layer via the transport-application interface to transport and translate valuable digital data into real-time vehicular applications such as automated steering control, lane change maneuvers, and brake application.

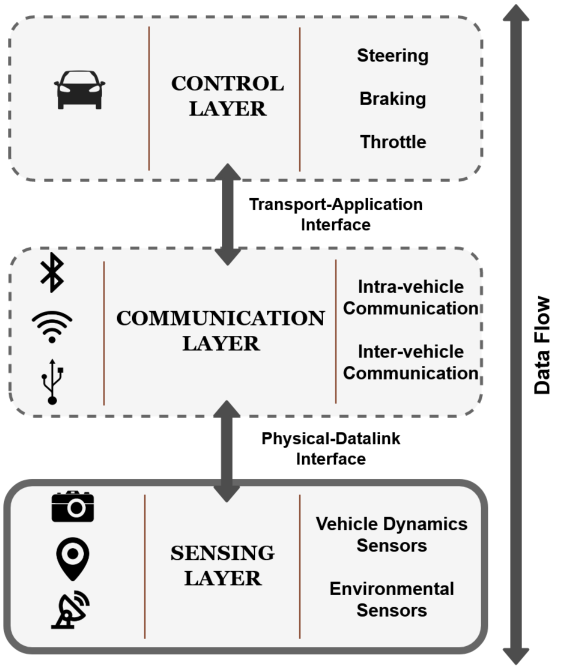


Fig. 1. Three-tier connected and automated vehicle architecture (AutoVSCC Framework).

B. Contribution

This paper focuses on vehicular cybersecurity threats targeting the sensing layer and is organized as follows: Section 2 provides an overview of the sensing layer, describing vehicular dynamics and environment sensors and its general protections and requirements to be met and secure sensing systems; Section 3 discusses attacks on vehicular dynamics sensors; Section 4 examines attacks on environment sensors; Sections 3 and 4 also provide existing countermeasures against vehicular sensor attacks; Section 5 offers potential futuristic solutions that rely on machine learning, Internet-of-Things, and blockchain technologies to secure vehicular sensors and Section 6 gives conclusions.

II. The Sensing Layer

A. Sensing Layer Overview

The vehicular sensing layer is comprised of vehicular sensors that measure the physical properties of a vehicle's state and surroundings. The sensing layer is critical to smooth vehicle operation since automotive electronic control systems use vehicular sensor measurements to make driving decisions [37]. For instance, distance sensor measurements allow adaptive cruise control systems to determine whether a vehicle can safely increase speed. In partially or fully automated vehicles, human sensing is replaced to some degree by vehicular sensing. Consequently, sensing layer data must have high reliability and accuracy.

The sensing layer contains anywhere from 60 to 100 sensors; however, as automakers work to increase vehicle automation, this number is expected to rise to as high as 200 [38]. Each of these sensors has a specific functionality. In [39], Abdelhamid *et al.* identify the different vehicular sensor functions like safety, diagnostics, convenience, and environment monitoring. Safety sensors provide night vision, detect impending crashes, and tailor airbag deployment to each passenger's weight and position. Diagnostic sensors detect vehicle malfunctions and offer malfunction alerts to drivers. Convenience sensors maintain high air quality within the vehicle, control automatic mirror dimming, perform automatic braking and acceleration, and adjust windshield wiper speed and temperature by detecting the presence of rain and fog. Environment monitoring sensors track the vehicle's surroundings, including traffic, street signage, and road conditions.

B. Environment Sensors and Vehicle Dynamics Sensors

Sensors within the sensing layer can be classified as either vehicle dynamics sensors or environment sensors, as shown in Fig. 2. Vehicle dynamics sensors measure the state of the vehicle, while environment sensors sense the vehicle's surroundings [40]. Most vehicle dynamics sensors are considered passive sensors, which are receivers, while most environment sensors are considered active sensors, which are both emitters and receivers [31]. The attack surface of an active sensor is, therefore, larger than that of a passive sensor, since attackers can target both signal reception and emission.

Environment sensors are used to detect parameters exterior to the vehicle. They detect objects in the immediate surroundings using Lidar, Camera, ultrasonic sensors, RADAR, and overall positioning using GPS receivers. All of the data obtained from environment sensors are used by the Driver Assistance System (DAS) to assist and increase the safe functioning of the vehicle. Vehicle dynamics sensors, on the other hand, are used to describe the vehicle's operation in 3D space (e.g., velocity, acceleration, and turn rates). It also includes in-vehicle telematics sensors like Tire Pressure Monitoring System (TPMS) and inertial sensors, which constitute the other in-vehicle running parameters. This paper focuses on critical sensors, where cyber-attacks have been demonstrated, and there is a need for detection methods and countermeasures to defend against them.

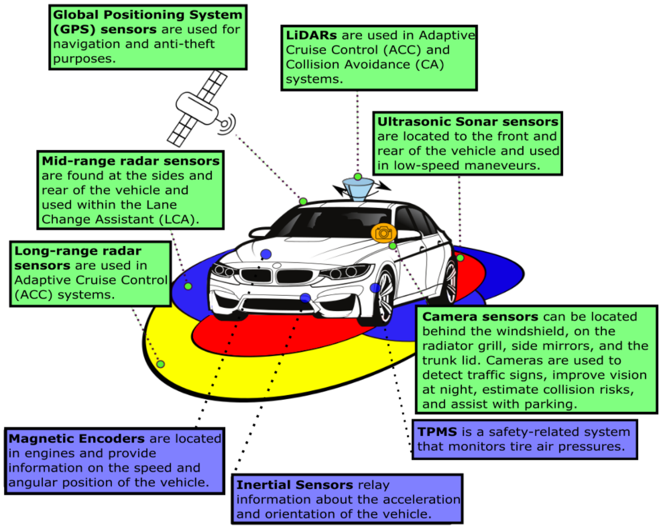

Global Positioning System (GPS) sensors are used for navigation and anti-theft purposes.
LiDARs are used in Adaptive Cruise Control (ACC) and Collision Avoidance (CA) systems.
Ultrasonic Sonar sensors are located to the front and rear of the vehicle and used in low-speed maneveurs.
Mid-range radar sensors are found at the sides and rear of the vehicle and used within the Lane Change Assistant (LCA).
Long-range radar sensors are used in Adaptive Cruise Control (ACC) systems.
Camera sensors can be located behind the windshield, on the radiator grill, side mirrors, and the trunk lid. Cameras are used to detect traffic signs, improve vision at night, estimate collision risks, and assist with parking.
Magnetic Encoders are located in engines and provide information on the speed and angular position of the vehicle.
TPMS is a safety-related system that monitors tire air pressures.
Inertial Sensors relay information about the acceleration and orientation of the vehicle.

Fig. 2. Vehicle dynamics sensors (Blue) and environment sensors (Green) in autonomous and connected vehicles.

C. Attack Vectors and Defenses

The sensing layer is vulnerable to malicious interference conducted both physically and remotely. Physical tampering requires an attacker to have direct access to the targeted vehicle. The attacker can then directly damage vehicle sensors or place materials that interfere with the sensor, such as electromagnetic actuators or sound-absorbent foam, onto the vehicle. Remote tampering can take the form of a roadside attack or a front/rear/side attack, as described by Petit *et. al.* [30]. In a roadside attack, an attacker places stationary attack equipment in one or more locations along the roadside. In a front/rear/side attack, attack equipment is mounted onto an attacker's vehicle. The attack can then be conducted as the attacker's vehicle follows, leads, or is side-by-side with the victim's vehicle. One other form of remote attack is the scenery attack described by Stottelaar [29], where an attacker manipulates the scenery by altering or duplicating traffic signs to deceive the vehicle sensors.

Remote tampering within the sensing layer has two attack vectors, identified by Shin *et al.* [31]. These are the regular and side channels. The regular channel is the physical interface through which the sensor receives input. This channel includes both sensor measurements and, in the case of active sensors, sensor emissions. The side channel consists of stimuli that are not the intended input signals but can be erroneously sensed by the sensor. These channels were originally identified in relation to sensor spoofing attacks; however, they also apply to the general exploitation of the sensing layer. Both physical and remote attack vectors are listed in Table I.

Ultimately, defenses against vehicular sensor exploitation must ensure that the following security requirements are met, as described by [41]:

1) Availability: Information collected by sensors should always be available, as vehicular sensors replace human

TABLE I
ATTACK VECTORS IN THE SENSING LAYER

Attack Vector	Access	Sensor Type	Description	References
Sensor Components	Physical	Active, Passive	Sensors can be physically tampered with or destroyed.	[21] [22] [23]
Receiver	Remote	Active, Passive	Attackers can transmit illegitimate signals to a sensor's receiver.	[24] [25] [26] [27]
Emitter	Remote	Active	Emitted signals can be eavesdropped and recorded.	[28] [29] [30]
Side Channel	Remote	Active, Passive	External stimuli can be directed at the sensor's transducer to disable sensor functionality.	[31] [32] [33] [34] [35] [36]

TABLE II
COMPARISON OF VEHICULAR SENSOR COUNTERMEASURES

Countermeasure	Complexity	Robustness	Primary Sensor(s)	Reference
Sensor Fusion	Medium-High	Medium	All	[42] [43]
Encryption using HSMs and PUFs	High	High	All	[18] [44]
Attack Detection	High	High	All	[31] [45] [46] [47]
Hardware/Software Modifications & Acoustic Filters	Low-Medium	Low	Inertial	[32] [35]
Static Code Analysis	Low-Medium	High	TPMS	[48] [17]
Random Probing	Low-Medium	Low	LiDAR	[49] [30]
Side Channel Modulation	Medium	Low	LiDAR	[50]
Physical Shift Authentication (PSA)	N/A	High	Ultrasonic	[27] [51]
Near-IR Light Filters	Low	Medium	Camera	[30]
Noise Filters	Medium-High	High	Radar	[52] [53] [54]
Sensor Threshold Monitoring	N/A	Low	GPS	[49]
Data Multi-routing	N/A	Low	GPS	[55]

observance and use the collected information to make decisions that have an impact on motorist and pedestrian lives.

2) Authorization: Only legitimate, authorized sensors must allowed to collect and distribute information on the status of the vehicle and the surrounding environment.
3) Confidentiality: Unauthorized nodes should not be able to decrypt sensor data.
4) Freshness: Sensor data should be collected frequently so that it is always up-to-date.
5) Integrity: As sensor data are being passed to other nodes, its information must not be changed.

Table II highlights defensive measures to secure various sensors in an autonomous vehicle. The complexity here is defined as the hardware and software resources required to implement the relevant countermeasure. A low complexity suggests minimal hardware/software requirements while a high complexity hints at more complex circuitry and advanced software. N/A implies that information for the corresponding countermeasure was not clearly specified in the references listed. The robustness of the countermeasure is determined by the number of attacks that can be mitigated by that countermeasure for a particular sensor. For instance, a single countermeasure can counter multiple attacks in the case of noise filters. Noise filters offer protection against jamming and spoofing/relay attacks and are thus considered as highly effective.

III. VEHICLE DYNAMICS SENSORS

Vehicle dynamics sensors such as magnetic encoders, inertial sensors, and Tire Pressure Monitoring Systems (TPMSs) provide measurements on a vehicle's state [40]. In this section, descriptions of attacks on vehicle dynamics sensors are provided. Protective measures that automakers can take to avoid and detect any malicious tampering of vehicular dynamics sensors are also discussed.

A. Magnetic Encoders

Magnetic encoders measure the angular velocity of a vehicle gear or wheel [56]. One type of magnetic encoder is the wheel speed sensor, which measures a wheel's rotational speed through the use of either magnetoresistance Integrated Circuits (ICs) or Hall ICs and is often used within Anti-Lock Braking Systems (ABS) [40]. Wheel speed sensors can also be used within indirect TPMSs, which use wheel speed sensors to calculate differences in rotational speeds and then estimate differences in pressure values [28].

1) Attacks:

- **Disruptive Attack:** During a disruptive attack, an attacker disrupts the magnetic field of the ABS's tone ring by placing an electromagnetic actuator between the wheel speed sensors, which are exposed underneath the vehicle body, and the ABS's tonewheel [24]. Shoukry *et al.* [24] note that disruptive attacks are not precise since the tone ring's magnetic field still plays a large role in determining the speed sensor's output.
- **Spoofing Attack:** Spoofing attacks occur when malicious actors gain unauthorized entry to a system and falsify information. To conduct a spoofing attack on wheel speed sensors, an attacker must first place an electromagnetic actuator between a wheel speed sensor and the ABS's tone wheel. The attacker then shields the original magnetic field so that the malicious magnetic field will have a significant effect on the output of speed sensor [24].

2) Countermeasures: In [56], Shoukry *et al.* argue that PyCRA (Physical Challenge-Response Authentication) can secure magnetic encoders or inductive active sensors. Traditional methods of cybersecurity include a query-response check or encryption algorithms, but in PyCRA, the authors propose security to sensors at a point prior to the digitization of the sensor response (i.e., the signal in its analog form). This is to make sure by laws of physics since an attacker cannot predict when the challenge is transmitted, as there will be a non-zero delay accompanying the attacker's response. In 2016, Shin *et al.* [31] successfully demonstrated PyCRA could be bypassed by using a low-cost microcontroller and advanced circuitry design. In this case, the sampling rate of an attacker is higher than that of the victim's sensor. After determining that PyCRA was not entirely secure [31], the authors of PyCRA also present some modifications [45] to PyCRA to detect and defend against magnetic encoder attacks. Shoukry *et al.* achieve a good degree of resilience against spoofing attacks by altering phases under low signal to noise ratio conditions.

B. Inertial Sensors

Inertial sensors consist of both acceleration sensors, more commonly known as accelerometers, and rotation-rate sensors, known as gyroscopes. Acceleration sensors measure the acceleration of the object to which they are attached. Rotation-rate sensors measure the rotation-rate with regard to a particular rotation axis [40].

1) Attacks:

- **Spoofing Attack:** Spoofing attacks on inertial sensors occur when malicious actors inject sound waves to deceive inertial sensors using "consumer-grade speakers or transducers, directivity horns, and amplifiers" [34]. Attackers can conduct two different types of spoofing attacks by manipulating injected analog signals to affect the resulting digital signal. Through side-swing attacks, attackers can strategically increase and decrease the injected waveform's amplitude to manipulate the vehicle's heading value [34]. During switching attacks, attackers alternate between injecting one waveform and another waveform of a different frequency to bring about phase pacing, which can cause the vehicle's heading value to continuously increase.
- **Acoustic Attack:** In an acoustic attack, attackers target spring-mass structures, such as Micro-Electrical-Mechanical Systems (MEMS) gyroscopes and accelerometers, which have a load resonant frequency [43]. They then falsify acoustic waves with a frequency matching the load resonant frequency of the cyber-physical system [57]. In [43], Nashimoto *et al.* details how acoustic attacks are carried by measuring inclination (roll, pitch, and yaw) parameters and evaluated by algorithms. Tu *et al.* [34] show that MEMS-based inertial sensors are vulnerable to acoustic attacks. Specifically, a case study was presented on how sampling drifts by ADC converters can contribute to such attacks. Son *et al.* [32] were able to successfully conduct acoustic attacks on gyroscopes within Unmanned Aerial Systems (UAS), and Trippel *et al.* [35] noted vulnerabilities to acoustic inputs within accelerometers.

2) Countermeasures: Son *et al.* [32] suggest creating a physical barrier against the noise, utilizing a differential comparator, or tuning the resonance frequency. Trippel *et al.* [35] propose several hardware design solutions like low-pass filter, secure amplifier, acoustic dampening materials, and software defense mechanisms (e.g., randomized sampling or 180 degrees out-of-phase sampling) to protect against an attacker's acoustic interference. Tu *et al.* [34] also suggest the use of isolators and dampeners, low-pass filtering, a dynamic sample rate, and sensor fusion.

C. Tire Pressure Monitoring Systems

TPMSs in use today include four pressure sensors for each tire, a TPM Electronic Control Unit (ECU), and a receiving unit [28]. The receiving unit, which in some cases is incorporated into the ECU, is able to collect packets sent by the TPMS pressure sensors within its vehicle or neighboring vehicles. These packets contain a sensor ID and pressure and temperature measurements. The TPMS discards packets whose sensor IDs do not correspond to any of the vehicle's tires.

1) Attacks:

- **Reverse-Engineering Attack:** In a reverse-engineering attack, attackers can deconstruct vehicular systems and reverse-engineer the vehicle firmware by extraction and modification in order to find vulnerabilities to carry out future attacks such as replay and relay attacks [58], [59]. Rouf *et al.* [28] were able to reverse-engineer the protocols used by two different TPMS sensors currently in use within automobiles. They did this through GNU's not Unix (GNU) Radio and the Universal Software Radio Peripheral.
- **Spoofing Attack:** When spoofing tire pressure sensors, attackers gain unauthorized entry to TPMSs and falsify tire pressure sensor measurements. If attackers can spoof tire pressure sensors, they can control the TPMS warning lamp and potentially cause drivers to stop their vehicles, putting vehicle occupants at risk of physical harm. Rouf *et al.* [28] were able to trigger a vehicle's low-pressure warning light and general-information warning light by using another vehicle on the highway to conduct a spoofing attack.
- **Eavesdropping Attack:** During an eavesdropping attack, attackers monitor sensor readings and transmissions. Eavesdropping threatens location privacy, as each TPMS sensor has a sensor ID that remains fixed for the duration of its lifetime. Rouf *et al.* [28] showed that it was possible to reach an eavesdropping range of up to 40 meters from a passing vehicle. They also showed that eavesdropping attacks on TPMSs are further facilitated because ECUs within TPMSs do not generally have authentication schemes in place to ensure that messages are coming from legitimate nodes.

2) Countermeasures: In [28], Rouf *et al.* suggest that TPMSs should incorporate basic error checking, detect when conflicting information has been received, and filter out false activation signals. They also argue that the current packet structure is not conducive to proper encryption, and thus, a sequence number field and a cryptographic checksum should be added to TPMS packets. In [60], Kilcoyne *et al.* propose a Linear-Feedback Shift Register (LFSR)-based encryption method that would shield sensor IDs from attackers. Feedback loops are recruited to create 64-bit encryption keys, thus making it robust against brute force attacks. This method utilizes XOR operations, which means that it brings with it minimal overhead. To combat eavesdropping attacks, Kolodgie *et al.* [61] suggest allowing TPMSs to broadcast only when the wheel is at an orientation that limits signal propagation. Amoozadeh *et al.* [62] and He *et al.* [63] propose the use of encryption with anonymity techniques (e.g., group signatures) and short-term certificates to preserve identity and location privacy on the usage data. The authors in [48] focus on the software for ECUs and suggest the use of static code analysis tools to identify and eliminate excess ambiguity in code design. These tools eliminate implementation flaws within the code that attackers can exploit by, for instance, the use of malware [17]. Checkoway *et al.* [36] recommend removing any "debugging symbols and error strings" from all code that is programmed onto an ECU.

IV. Environment Sensors

Environment sensors provide measurements relating to vehicular surroundings and include Light Image Detection and Ranging (LiDAR) systems, ultrasonic sensors, cameras, Radio Detection and Ranging (Radar) systems, and Global Positioning System (GPS) sensors [40]. This section discusses the cyber-attacks to which environment sensors are vulnerable. Countermeasures against environment sensor attacks are also presented.

A. LiDAR

Light Imaging Detection and Ranging (LiDAR) systems rely on laser scanning techniques to generate a three-dimensional mapping of their surroundings [30]. LiDAR systems can be of scanning or solid-state types [25]. In scanning LiDARs, one or more laser transceivers are rotated, while solid-state LiDARs can map without relying on rotation. Scanning LiDARs are the primary type of LiDAR used today; however, in the future, solid-state LiDARs will dominate the market. Scanning LiDARs can map a vehicle's surroundings by sending out laser pulses while rotating. When these pulses meet with surrounding objects, they are then reflected back to the LiDAR. These reflected pulses are known as echoes. A single laser pulse may generate several echoes if the pulse is not completely stopped when reaching an object. The LiDAR can then calculate its distance to the obstacle using the speed of light and the time between pulse transmission and reception of the echo. As the LiDAR spins, it eventually generates a three-dimensional, three hundred and sixty-degree view of the obstacles that are nearby. This functionality is relied upon by Adaptive Cruise Control (ACC) and Collision Avoidance systems [30].

1) Attacks:

- **Replay Attack:** Attackers can receive and record signals sent by the LiDAR. At a later point in time, the attackers can conduct a replay attack by sending the recorded signals back to the LiDAR in order to cause the LiDAR to map non-existent objects [29].
- **Relay Attack:** Replay attacks can be extended in order to carry out a relay attack, which can disrupt the LiDAR's ability to accurately gauge the distances of nearby objects. During a relay attack, attackers receive LiDAR signals and transmit those signals to a receiver in a different location. The second receiver can then send the signals back to the LiDAR leading to an incorrect map location of nearby objects [30].
- **Blinding Attack:** Blinding attacks are carried by injecting a light source of the same wavelength as the LiDAR's pulses. The external light source will cause the LiDAR to experience saturation, which would effectively deny its services to the vehicle. LiDARs transmit infrared light pulses, so the attacker's light source must have to be infrared light. As infrared light is not detectable by the human eye, blinding attacks can occur without the vehicle's occupants' knowledge [25].
- **Spoofing Attack :** Spoofing attacks cause LiDARs to detect non-existent objects. In [30], Petit *et al.* were able to spoof a LiDAR system and cause it to over-calculate its distance to an obstacle. Shin *et al.* [25] discuses a spoofing attack on a LiDAR system; however, their Attack could also force the LiDAR to under-calculate the distance to an obstacle.
- **Jamming Attack:** This type of Attack directly emits light back at the scanner unit on the vehicle that uses the same frequency band as the laser [49]. The author in [64] points out a low-cost, off-the-shelf system using a Raspberry Pi and a low-power laser to jam the LiDAR sensor of a vehicle.
- **Denial-of-Service Attack:** Attackers can conduct denial of service attacks on LiDARS by injecting an enormous number of fake objects created using by jamming or spoofing [29]. If the number of injected objects is larger than the maximum number of objects that a LiDAR can track, then the system becomes unstable.

2) Countermeasures: Though general defenses against spoofing and jamming may also decrease the likelihood of a replay or relay attack occurring, few studies have been dedicated to specifically examining replay and relay attack prevention.

Matsumara *et al.* [50] offer an approach that guards against spoofing by modulating the LiDAR laser with side-channel information, thereby preventing attackers from injecting false reflection signals since they do not know the side channel's secret key. Petit *et al.* [30] suggest that LiDARS could utilize signals of different wavelengths so that the attacker will have difficulty in targeting multiple wavelengths simultaneously. Additionally, LiDARs could incorporate random probing [49] by varying the time interval between laser pulses. This will prevent attackers from being able to predict when they should inject fake pulses so that the pulses are reached within the interval. Random probing could also occur by skipping some pulses. If the LiDAR notices incoming pulses during these skipped intervals, it can be aware that an attacker is potentially targeting the vehicle. The pulse period can also be shortened, thereby shortening the attack window. In [30] and [65], LiDARs are shown to probe more than once in order to detect random jamming and thus to shorten the pulse period to lower the attack window.

Denial-of-service attacks can be prevented by increasing the number of objects that are tracked at one time by the LiDAR sensor. [29].

B. Ultrasonic Sensor

Ultrasonic sensors can detect nearby obstacles and calculate their distance to the vehicle [27]. The sensor emits an ultrasonic signal to detect nearby objects, which, upon reaching an obstacle, will be reflected back to the sensor. The time between the transmission of the signal and the reception of the reflected signal can then be used to calculate the distance of the obstacle to the vehicle. Ultrasonic sensors are often used to assist drivers in conducting tasks that are typically at very low speed (e.g., parking) [40].

1) Attacks:

- **Blind Spot Exploitation Attack:** Lim *et al.* [21] found that a vehicle's ultrasonic sensors cannot detect very thin objects in their blind spot region. Attackers can take advantage of this vulnerability by placing a thin object in a reversing vehicle's blind spot so that the vehicle can collide with the object.
- **Sensor Interference Attack:** Attackers can conduct sensor interference attacks to interfere with the legitimate sensor's measurements by placing their own ultrasonic sensors opposite to a vehicle's ultrasonic sensors [21]. When two sensors are placed opposite to each other, each sensor will receive the other sensor's signals in addition to its own reflected signals.
- **Cloaking Attack :** Attackers conduct cloaking attacks in order to conceal the presence of nearby objects from the ultrasonic sensor [26]. To conduct a cloaking attack, attackers can simply place sound-absorbent materials around obstacles so that the sensor does not detect them. In [21], Lim *et al.* were able to conceal objects covered with acoustic foam from an ultrasonic sensor.
- **Physical Tampering Attack:** Attackers can physically tamper with an ultrasonic sensor's receiver and transmitter by covering them. Lim *et al.* [21] were able to disable the functionality of an ultrasonic sensor by covering its receiver and transmitter with scotch tape. Attackers can use this technique to cause ultrasonic sensor failure.
- **Acoustic Cancellation Attack:** Acoustic cancellation attacks can be used to eliminate legitimate ultrasonic signals. Attackers can cause an ultrasonic signal's phase to become zero by transmitting an illegitimate signal with a phase opposite to the legitimate signal [51]. This type of attack requires resources that would mostly be available to experience and knowledgeable attackers and is thus more difficult to conduct than a cloaking attack.
- **Spoofing Attack:** Three types of spoofing attacks are possible: simple, random, and advanced. During simple spoofing attacks, attackers direct ultrasonic signals toward an ultrasonic sensor. The false signals may be able to reach the ultrasonic sensor before the legitimate, reflected signals emitted from the sensor itself and thus may falsely perceive a non-existent object [26]. During a random spoofing attack, a legitimate ultrasonic signal is pre-recorded and then randomly resent to the ultrasonic sensor in a continuous mode. In the advanced spoofing attack, an attacker listens for an incoming ultrasonic signal, eliminates the reflected signal by a cloaking attack, and sends a falsified reflected signal back to the ultrasonic sensor [27].
- **Jamming Attack:** Jamming attacks occur when an attacker continually sends ultrasound pulses in the direction of an ultrasonic sensor [26]. The sensor is then overwhelmed and unable to accurately gauge the vehicle's distance to nearby objects [51]. In [27], Xu *et al.* were able to perform a jamming attack on a Tesla Model S vehicle in the self-driving Autopark and Summon modes which caused the vehicle to collide with undetected obstacles.

2) Countermeasures:

To counter blind spot exploitation, sensor interference, and cloaking attacks, Lim *et al.* [21] suggest utilizing sensor fusion and backup cameras in order to verify the legitimacy and accuracy of ultrasonic sensor measurements. The authors also suggest calibrating sensors immediately after starting the vehicle in order to prevent sensor tampering attacks. Futuristic algorithms require an extensive collection of real-time navigational data (i.e., from 360 degrees sensors) for training and testing blind spot detection models. Specifically, models that integrate 3D-CAD geometry of vehicles along with advanced computer vision approaches (i.e., instance segmentation, color edge detection, and background elimination) has the potential to improve the real-time detection rate of blind spot areas.

Though defenses against acoustic cancellation attacks are scant, several anti-spoofing and jamming techniques have been presented. Physical Shift Authentication (PSA) [27] is one defense against simple spoofing, random spoofing, advanced spoofing, and jamming attacks. PSA randomizes the waveforms of the ultrasonic signal. The reflected signals will only be accepted if they correlate to the randomized waveform. The ultrasonic signal frequency is also continually changed to prevent jamming attacks. Lee *et al.* [51] propose a similar strategy that estimates the width of an incoming pulse and rejects any incoming signals with suspicious pulse widths. Multiple Sensor Consistency Check (MSCC) [27] is a method that relies on sensor redundancy to counter jamming and spoofing attacks. MSCC can locate attackers and has the ability to verify sensor measurements. In MSCC, a sensor transmits its measurements to several other sensors to validate measurements.

C. Camera

Within automated vehicles, cameras are necessary so that the vehicular system can identify its surroundings [26]. These sensors are used for purposes such as detecting traffic signs, identifying hard-to-see objects during the night-time, showing drivers nearby obstacles while they are parking, avoiding collisions by using sensor data to track nearby objects and checking the validity of information gained from other sensors [40].

1) Attacks:

- **Blinding Attack:** Blinding attacks disable the functionality of the vehicle's camera sensors. A strong laser beam focused at the camera leads to higher tonal values, and the attacker exploits this phenomenon to conceal the camera feed, causing complete blindness to the vehicular sensory inputs [30]. This may lead to vehicle distortion or even emergency braking [26], [30].
- **Auto-Control Attack:** Auto-control attacks also target camera sensors. Attackers continually direct bursts of light at the camera in an attempt to manipulate the auto controls so that the image cannot stabilize. This type of attack can generally only be implemented in what [30] terms as a front/rear/side attack.

2) Countermeasures: Petit *et al.* [30] offer several suggestions to guard against blinding and auto-control attacks on cameras. They advocate incorporating multiple cameras with the same view and near-infrared light filters capable of eliminating infrared light interference during daylight hours. They also propose the use of photochromic lenses, which can filter certain wavelengths of light. To mitigate any consequences due to a camera's blind spots, Rangesh & Trivedi [66] test a method that uses a "full-surround" Multi-Object Tracking (MOT) framework to track objects in real-time using early fusion and ground-truth images. Early fusion combines all instances or proposals of a particular object in the blind spot at the start of each tracking operation. These proposals are then fed through an MOT framework based on the Markov Decision Process (MDP) and reinforcement learning to notify the driver if an object is detected.

D. Radar

Radio Detection and Ranging (Radar) sensors emit electromagnetic signals and gauge the distance of nearby objects by determining the time elapsed from the moment the signal is sent to the moment the signal is detected by the radar's receiver. Most radar sensors today operate within the millimeter wave (mmW) frequency band [65]. Long-range radar sensors are used in Adaptive Cruise Control (ACC), mid-range radar sensors are used as part of Lane Change Assistants (LCA), and short-range radar sensors are used to alert drivers of potential obstacles while they are parking their cars [40].

1) Attacks:

- **Jamming Attack:** During jamming attacks, attackers can jam radar sensors with a signal that is a part of the same frequency band [13], [26]. Signal jamming can lower the sensor's signal to noise ratio, which can cause the radar system to lose the ability to detect nearby objects [26].
- **Spoofing/Relay Attack** Spoofing/Relay attacks occur when malicious actors falsify signals and continually retransmitting a previous legitimate signal. Attackers can use a Digital Radio Frequency Memory (DRFM) repeater to store a signal, create a digital duplicate, and then continually retransmit the duplicate so that the radar will consider it to be a legitimate signal [13], [67].

2) Countermeasures: Yan *et al.* [26] suggest incorporating data fusion and attack detection. In [52], Lu *et al.* presented a filtering method that combats DRFM signals and would prevent both jamming and spoofing/relay attacks carried out using a DRFM repeater. Dutta *et al.* [53], present a hybrid filter that uses the modified Kalman filter and a Chi-squared detector to detect false data that is injected at random points and minimize the impact this data will have on radar sensor inputs. The authors in [54] use a novel Spatio-Temporal Challenge-Response (STCR) approach to detect and mitigate spoofing attacks by using a MIMO antenna and multiple beamforming to constantly probe the environment with signals in several directions and detecting the reflected signals. If the reflected signals exceed a noise threshold, they are considered malicious and are excluded from distance calculation.

E. GPS

Connected and automated vehicles utilize the Global Positioning System (GPS) to obtain their location identity and geographic location. GPS satellites send navigation messages to on-ground receivers, which then calculate their distance to satellites by using the message's time of transmission and arrival. Receivers can determine their location by calculating their distance to at least four different satellites. However, since these receivers do not authenticate or encrypt signals and since the spreading codes used within GPS are public knowledge since GPS is an open standard with a transparent architecture [49], GPS communication is vulnerable to attack [68]. As automated vehicles depend upon GPS, [67] considers attacks on GPS systems within automated vehicles to be, along with attacks on the camera sensor, the highest priority in terms of automated vehicle cybersecurity.

1) Attacks:

- **Jamming Attack:** During a GPS jamming attack, GPS sensor signals are jammed to prevent locating the vehicle. Petit and Shladover [67] argue that GPS jamming is one of the simplest attacks as GPS jammers are cheap and widely available. If enough radio noise is added to the GPS signal at the operating frequency (e.g., 1575.42 MHz), the receiver in the vehicle cannot distinguish the authentic signal.
- **Spoofing Attack:** Spoofing attacks occur when an attacker takes advantage of GPS signals' low power and supplies a false GPS signal with higher signal strength to overpower the original signal and compromise data integrity [68]. Attackers can either tamper with the GPS receiver so that it computes false locations and times [13], [58] or transmit data to interrupt the GPS receiver as it attempts to communicate with GPS satellites, thereby preventing the receiver from locating its position.

Spoofing attacks can be used as a first step in conducting additional attacks, including replay and tunnel attacks [69], [70].

- **Black Hole Attack:** In a black hole attack, an attacker deliberately causes the loss of information that was supposed to be forwarded from one vehicle to another. This type of attack occurs within self-organized Vehicular Ad hoc NETworks (VANETs) made of nodes that consist of either vehicles or road-side infrastructure. [71].

  To conduct a black hole attack, attackers can falsify their GPS data and advertise themselves as having the shortest path to the destination node. Routing protocols such as Link State Routing (LSR) and Ad-hoc On-demand Distance Vector (AODV) would then allow them to reply to the route request message since this privilege is given to the nodes with the shortest path to the destination node [55]. The malicious node can then drop the relevant packets ensuring that information does not reach the destination node. Blackhole attacks can eventually crash the network topology. One variant of black hole attacks, called gray hole attacks, occur when attackers alternate between normal behavior and randomly dropping packets. Gray hole attacks are especially difficult to detect.

2) Countermeasures: To combat GPS jamming attacks, Petit and Shladover [67] suggest incorporating inertial sensor measurements in the case of jamming attacks. Khanafseh *et al.* [72] develop Receiver Autonomous Integrity Monitoring (RAIM) detection using measurements from both the GPS and the vehicle's Inertial Navigation System (INS), which is comprised of inertial sensors. Additionally, the authors in [49], [73] suggest the use of a secondary source or hybrid navigation system for GPS signals such as the European Union's Galileo or India's Indian Regional Navigation Satellite System (IRNSS) also called as NAVIC.

To defend against GPS spoofing attacks, Liu *et al.* [74] examine the effects of spoofing attacks on combined INS and GPS systems and advocate for an integrated system. Psiaki and Humphreys [75] uses signal encryption, analysis of drift, analysis of incoming signal direction, or hybrid. Bittl *et al.* [69] provide countermeasures that would secure time tracking, lower the lifespan of pseudonym certificates, and log changes in timing. Other countermeasures for GPS spoofing, as highlighted by Parkinson *et al.* [49], include 1) the use of validation mechanisms such as monitoring GPS signals to ensure that any relative changes are within a threshold, and 2) GPS signal strength varies as expected within a range. Ideally, the authors state that a cryptographic and military-grade implementation of a GPS system is the foolproof solution to spoofing.

As for black hole attacks, Mahmood and Khan [55] suggest building multiple routes to the destination node. Road-Side Units (RSUs) and associated transportation infrastructure can aid in detecting black hole attacks.

V. Future Outlook

A future for autonomous vehicles is quite promising as the automotive industry is racing to provide comfort and safety. As research and development of fully autonomous vehicles are underway, intelligent sensors will play a major role in determining how well these autonomous vehicles run on roads. As each vehicle may contain over 200 sensors with an intelligent onboard infotainment system and state-of-the-art cloud-based telematics, data privacy and security are critical for vehicle manufacturers, vendors, and customers [96]. As cyber-attacks become a method of warfare, innovative technologies such as machine learning and blockchain will play a significant role in offering cybersecurity solutions.

A. Recommendations

An IEEE report provides a complete list of recommendations to address cyber threats under six dimensions that interconnects AI and ML to cybersecurity: 1) legal and policy perspective; 2) human factors; 3) new frontiers on data handling; 4) hardware platforms; 5) software algorithms, and 6) operationalization [97]. The evolving applications of AI and ML to vehicular networks (Vehicle-to-Vehicle (V2V)/Vehicle-to-Infrastructure (V2I)) present a new set of challenges and risks compared to conventional approaches. The automotive OEMs should be prepared to overcome adverse, disruptive, and even catastrophic incidents when these technologies are deployed in the field. They will need to address any legal and liability mechanisms and develop policies quickly by working with relevant stakeholders that contain technical feedback loops to regulators, industries, government, national labs, and non-profit entities. Currently, there is a lack of regulatory bodies to oversee any malfunctions or inadequate care deployment of ML/AI approaches.

This calls for the creation of a coordinated data warehouse that is sponsored by governments and industries like the Waymo Open Dataset which consists of high resolution, independently-generated 3D labels for LiDAR sensors and 2D labels for camera data. Such data warehouses should enable new pathways to national or global standards to address feature engineering, computing, and storage. Security researchers need to consider factors such as Relevancy, Confidentiality, Integrity, and Availability (RCIA) during their training of any futuristic AI/ML models for vehicular interfaces. As the scale of real-world data available for training ML/AI models and the number of parameters in these models increases, they will be able to encapsulate realistic scenarios and provide repeatable and robust performance in large, complex environments [98].

B. Latest Trends

Depth perception in autonomous vehicles is typically done by hardware LiDAR that produces a 3D point cloud representation of the environment [99]. Recently, pseudo LiDAR approaches based on deep learning are gaining attention as they can generate per-pixel depth maps of surrounding environments from camera inputs [100]. There is currently a debate within the autonomous vehicle community on whether a hardware LiDAR, which is more accurate and expensive, can replace a pseudo-LiDAR, which has lower hardware and higher computation costs. Notably, the cybersecurity strategy for vehicular sensors would be significantly different for hardware and pseudo LiDARs.

TABLE III
ROLE OF EMERGING TECHNOLOGIES IN VEHICULAR SECURITY

Technology	Primary Utility	Property	Reference
Machine Learning	Intrusion/Malware Detection on ECUs	Confidentiality, Availability	[76] [77] [78] [79] [80] [81] [82] [83] [84]
Blockchain	Secure Platform for Data Dissemination	Integrity, Confidentiality	[65] [16] [85] [86] [87] [88]
Quantum/Post-Quantum Cryptography	Entropy/Non-Entropy Cryptography for ECUs	Integrity, Availability	[89] [90] [91]
Machine Learning in IoT	Edge & Cloud-Based Intrusion Detection	Confidentiality, Integrity, Availability	[92] [93] [94]
Lightweight Cryptography	Data Encryption for IoT Systems	Confidentiality	[95]

Computer architectures used in autonomous vehicles have to deal with two different workloads. The sensory and perception modules that use machine learning and deep learning models need relatively simpler calculations (e.g., matrix multiplication) on very large data sets. On the other hand, the planning and control modules require relatively complex computations (e.g., iterative optimization) on smaller data sets [97]. Also, studies have pointed out that data handling takes a larger time than actual data processing [97]. This calls for new architectures or platforms that run on large data repository or warehouses in real-time to monitor and track vehicular network states. Recently, computer architectures capable of dealing with the sensory load from autonomous vehicles have been commercialized and deployed in passenger vehicles (e.g., NVIDIA DRIVE AGX, Tesla FSD Hardware 3.0). Table III features the most recent work done in these technologies and lists the role of emerging technologies in securing vehicular sensors and their data.

C. Machine Learning Based Solutions

Machine learning techniques are being deployed in autonomous vehicles so that vehicular systems can make appropriate and safe choices based on learned experience rather than fixed rules. Machine learning algorithms can also be used for intrusion detection systems to recognize patterns of normal behavior and issue alerts when abnormalities occur [20], [78], [80], [81]. For instance, the authors in [77] use a supervised learning Deep Neural Network (DNN) model that can be deployed on ECUs to monitor sensor inputs based on trained traits of attacks and profiles incoming inputs as a 0's (non-malicious) or 1's (malicious) to its existing attack identification model and notifies the system to take appropriate responses. The DNN model was tested on a TPMS and claimed to achieve 99.9% accuracy in detecting malicious packets and a false negative percentage of 0.2%.

The authors of [76], [79], [82], and [83] provide applications of machine learning to detect attacks against vehicular sensors and provide a recommendation to the driver, the use of deep learning for detecting unforeseen objects, the elimination of software vulnerabilities present in the large software code bases in automotive systems at an early stage in the software development lifecycle using deep learning, and detection of malware in x86-based devices that are prevalent in autonomous systems respectively.

The Internet-of-Things, coupled with data-driven machine learning algorithms, will certainly add several cyber threats that will intrude vehicular networks and fog nodes on cloud layers. The authors in [92] argue the need for unsupervised clustering association-based methods to handle the Data Deluge (DD) problem for next-generation cyber-resilient systems. Specifically, they developed an intrusion algorithm that relies on a Software Defined Radio (SDR) model achieving an accuracy of 99.7%. Similar methods need to be tested with vehicular network data sets.

Machine learning can be deployed on low-resource hardware such as ECUs by considering the field of TinyML. Typically designed for edge systems such as mobile devices, TinyML is expanding its scope to consider hardware which is tightly constrained. The authors in [84] suggest the potential for machine learning models such as DNN, Decision Tree, and SVM (Support Vector Machine) to be deployed on hardware that gathers telemetry data from sensors. However, traditional hardware benchmarks currently used in machine learning cannot accurately gauge the performance for smaller, less powerful hardware, and as such, benchmarking techniques are currently being explored [101].

Machine learning models also suffer from several limitations: 1) limited access to large labeled (annotated) data sets; 2) extensive training times; 3) probability of high false-positive rates with no human input; 4) scalability and real-time deployment issues, and 5) access to heterogeneous test data for cross-validation. Also, autonomous vehicles are usually ill-equipped to bear the high computational workloads generated by these AI models [82]. The models also need to be trained under uncertain environments such as left/right turns, blind-spot detection, collision avoidance, and weather conditions [76]. Sharma *et al.* [102] have demonstrated that ML models can be a disruptive technology to attack autonomous vehicles. In this work, four machine learning algorithms are first trained on normal data and then tested on model-generated “fake' data. It was found that about 14% (low accuracy) of the data was misidentified by these algorithms. The authors do state that with increased access to real-world vehicular datasets, the ML models can be better trained to identify fake data.

D. Blockchain Based Solutions

Though the adoption of the Internet of Things (IoT) in vehicular networks is on the rise, there are still major challenges such as scalability, security, lack of standards, centralized networks, architecture models, and cost [103]. A distributed platform or Distributed Ledger Technology (DLT) such as blockchain has the potential to overcome

TABLE IV
APPLICATIONS AND CONSTRAINTS OF BLOCKCHAIN USAGE IN IoV NETWORKS

Application	Attack	Defense	Challenges	References
Trust Management & Announcement Network in VANETs	Spoofing, Replay, MITM	Bayesian Rating, PKI, Unique IDs, Consensus Algorithms, Verification & Validation	Data Privacy	[105] [106] [107] [108]
Message Handling	DoS, DDoS	PKI, Event Message Authentication	Overhead & Latency	[16] [109]
ECU Data Storage & Local/Regional Blockchain, SDVN	Spoofing (Immutability), DoS Eavesdropping	ACL, Symmetric Encryption, Reduce Delay	Cloud Reliance	[110] [81] [82]

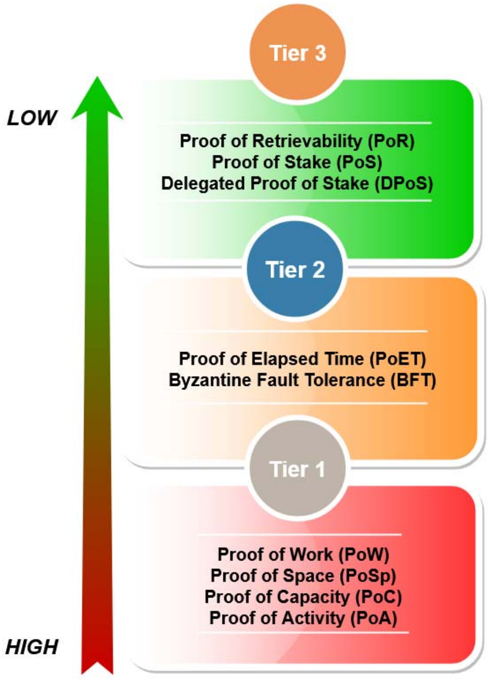


Fig. 3. Hierarchy-based consensus algorithms for blockchains in vehicular environments.

these challenges and to increase the protection against vehicular cyber-attacks [104].

The most important characteristic features of the blockchain are immutability (tamper-proof) [104], distributed networks (peer-to-peer operations) [105], security and privacy (through asymmetric cryptography) [111], and anonymity (keeping participants' identities undisclosed) [112]. Blockchain-based solutions can be effectively used for providing real-time information and making transactions between various stakeholders of the automobile industry, such as manufacturers, customers, auto financing companies, service providers, and insurers. Moreover, sensor data from various units of each vehicle or V2V or V2X can be integrated within the blockchain as 'blocks' using consensus algorithms. Consensus algorithms are mechanisms where participating nodes within the blockchain network reach a collective agreement on the addition of new blocks. These blocks can then be used to make real-time decisions for applications or use cases such as optimal navigation path-finding, avoiding obstacles, and following relevant traffic signs. Fig. 3 presents a collection of consensus-based algorithms in vehicular environments. The consensus algorithms are organized into three tiers based on existing literature [113]–[115]. For example, tier 3 algorithms are considered to have low requirements in terms of processing time, handling the number of transactions, costs, and resource-sharing [116]. Conversely, tier 1 and tier 2 algorithms demand moderate to higher computational resources, larger latencies, and higher costs [117]. To deploy BC for vehicular applications, tier 3 algorithms are preferred over tiers one and two.

Table IV lists applications and constraints of using the blockchain technology in vehicular environments along with the attacks and mitigation tactics for each application. Privacy in the vehicular environment refers to safeguarding the identity of vehicles or RSUs during interaction and communication exchanges with other vehicles or infrastructure. While securing the identities of participating vehicles are critical, the overhead costs of communication for enabling authentication come at a larger price. So, finding a trade-off among right key sizes, frequency of dynamic key management of public/private keys, and modifying vehicle/session IDs is a challenge to avoid leakage of sensitive data (i.e., to preserve privacy).

Communication overhead & latency refers to finding an optimal cost that the distributed network can handle at any given time during send/receive requests and processing of such requests. To avoid large communication overhead, the futuristic architecture of the blockchain must be lightweight and yet contain secure properties.

As participating vehicles scale within distributed VANETs, the additional computational burden will increase the overhead costs, thus limiting the network performance (i.e., throughput and bandwidth). Cloud architectures offer some potential in implementing a truly distributed BC architecture but finding an optimal balance among several parameters (i.e., latency, overhead costs, network performance, and privacy-preservation) is a challenge.

Some common and potential promising communication technology for BC where vehicles can connect to each other are 5G, Dedicated Short Range Communication (DSRC), and cellular communications. These technologies offer benefits such as low latency, high throughput, and affordability and are suitable to scale well in vehicular applications. DSRC, specifically, does not have any infrastructure set-up expenses [118].

1) Blockchain-Based Applications in Inter-Vehicle Networks (V2X):

Blockchain technology can also be used to implement secure, remote software or OTA updates for ECUs (Electronic Control Units) in autonomous vehicles. ECUs contain lookup

TABLE V
VEHICULAR STANDARDS FOR AUTOMOTIVE SECURITY

Standard Name	Organization	Standard Number	Reference
Threats, Vulnerabilities and Risk Assessment	ETSI	ETSI TR 102 893	[119]
ITS Communications Security Architecture and Security Management	ETSI	ETSI TS 102 940	[120]
IEEE Standard for Wireless Access in Vehicular Environments	IEEE-SA	IEEE 1609.2-2016	[121]
Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related System	IEC	IEC 61508	[122]
Electrical and Electronic Components and General System Aspects	ISO	ISO/TC 22/SC 32	[123]
Road Vehicles — Functional Safety	ISO	ISO 26262	[124]
Road Vehicles — Cybersecurity Engineering	ISO	ISO/SAE DIS 21434	[125]

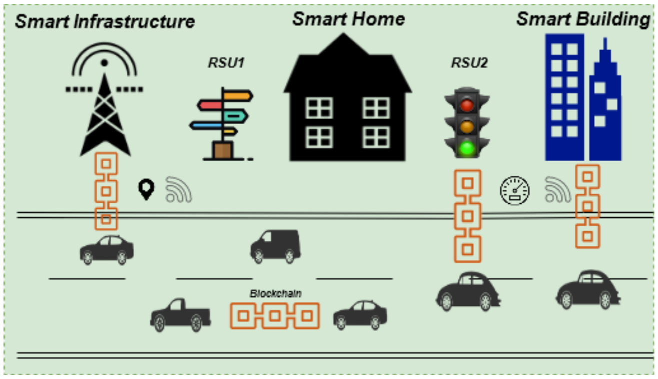


Fig. 4. Blockchain implementation to secure V2X data from vehicles.

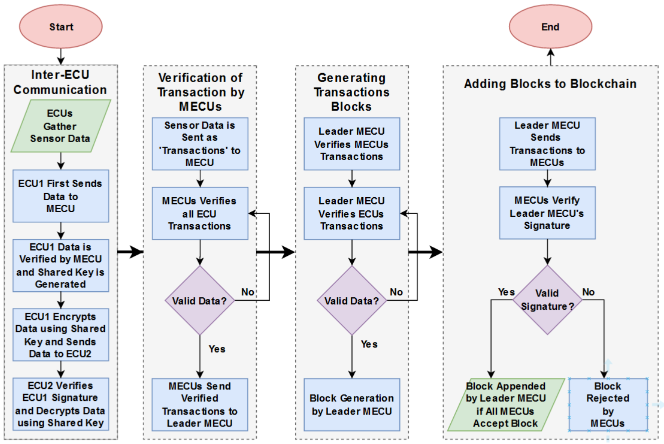

Start
End
Inter-ECU Communication
ECUs Gather Sensor Data
ECU1 First Sends Data to MECU
ECU1 Data is Verified by MECU and Shared Key is Generated
ECU1 Encrypts Data using Shared Key and Sends Data to ECU2
ECU2 Verifies ECU1 Signature and Decrypts Data using Shared Key
Verification of Transaction by MECUs
Sensor Data is Sent as 'Transactions' to MECU
MECUs Verifies all ECU Transactions
Valid Data?
No
Yes
MECUs Send Verified Transactions to Leader MECU
Generating Transactions Blocks
Leader MECU Verifies MECUs Transactions
Leader MECU Verifies ECUs Transactions
Valid Data?
No
Yes
Block Generation by Leader MECU
Adding Blocks to Blockchain
Leader MECU Sends Transactions to MECUs
MECUs Verify Leader MECU's Signature
Valid Signature?
Yes
No
Block Appended by Leader MECU if All MECUs Accept Block
Block Rejected by MECUs

Fig. 5. Blockchain implementation to secure intra-vehicular data from ECUs [86].

tables that hold the maximum, minimum, and average values for the outputs of relevant sensors. The ECU's software interprets this data and sends actionable commands to the sensors for optimal performance [65]. Dorri *et al.* [16] implement an overlay blockchain network of nodes that consist of smart vehicles, buildings, OEMs, smartphones, etc. Strong authentication, integrity, and confidentiality of the participating nodes are maintained due to the usage of hashes and Public Key Infrastructure (PKI) [126]. However, the authors also list the shortcomings of this implementation, such as its susceptibility to DDoS attacks and the release of spoofed updates by attackers. Fig. 4 highlights a blockchain-based infrastructure to handle V2X communications.

2) Blockchain-Based Applications in Intra-Vehicle Networks: Shrestha and Nam [110] developed a blockchain environment for information exchange in VANETS based on a geographic location. Data from the GPS and other sensor parameters are some example types of information that can be exchanged using blockchain among participating nodes (i.e., RSUs). Incidents such as accidents and traffic jams can be other messages that vehicles can share using a blockchain network. The authors claim that such a blockchain network is susceptible to what's known as an "immutability attack" (a form of spoofing), where malicious vehicles on the network have the ability to manipulate or modify the data, specifically when their collective computational power exceeds that of the victim vehicles. This attack can be mitigated by reducing delays during message delivery (i.e., access to high bandwidth environment) among benign vehicles and the utility of cloud computing among RSUs.

Alam *et al.* [86] propose a blockchain-based solution to secure ECU data, as shown in Fig. 5. The read and write operations by ECUs and other sensors inside each vehicle are relayed to domain controllers called 'Mother ECUs' (MECUs). MECUs are computationally more powerful than regular ECUs. The connectivity between ECUs and MECUs is established through vehicle communication buses (i.e., CAN and FlexRay protocols). Identity-based access control and verification are also implemented for inter-ECU communications. This is a security measure to enforce the principle of least privilege [127]. Attacks based on injection or falsification of data are rendered ineffective due to multi-tier integrity checks based on block hashes and ECU/MECU signatures.

Wagner and McMillin [107] call for a platoon-based blockchain implementation to secure data that is exchanged by vehicles without the need for RSUs or infrastructure to relay/store vehicular data. Transactions in this blockchain are issued in blocks on the blockchain network to primarily verify the integrity of the data that is being exchanged on the peer-to-peer network. This data is a cyber representation of the physical actions being carried out by other vehicles on the network (such as a lane change). This blockchain implementation is secure against bogus information attacks, as a malicious or faulty member can intentionally or unintentionally (via sensor faults) relay incorrect information to the blockchain.

E. Compliance and Regulation

The attacks, countermeasures, and future developments reviewed in this paper can be integrated with industry-level

TABLE VI
NOMENCLATURE

Acronym	Definition
ABS	Anti-Lock Brake System
ACC	Adaptive Cruise Control
ACL	Access Control List
AODV	Ad-Hoc On-Demand Distance Vector
AutoVSCC	Autonomous Vehicular Sensing Communication and Control
BFT	Byzantine Fault Tolerance
CPS	Cyber-Physical System
DDoS	Distributed denial-of-service
DAS	Driver Assistance System
DLT	Distributed Ledger Technology
DNN	Deep Neural Network
DRFM	Digital Radio Frequency Memory
DSRC	Dedicated Short Range Communications
ECU	Electronic Control Unit
ETSI	European Telecommunications Standards Institute
GNU	GNU's Not Unix
GPS	Global Positioning System
HSM	Hardware Security Module
IC	Integrated Circuit
IEC	International Electrotechnical Commission
INS	Inertial Navigation System
IoT	Internet of Things
IRNSS	Indian Regional Navigation Satellite System
ISO	International Organization for Standardization
ITS	Intelligent Transportation System
LCA	Lane Change Assistants
LFSR	Linear-Feedback Shift Register
LiDAR	Light Image Detection and Ranging
LSR	Link State Routing
MEMS	Micro-Electrical Mechanical Systems
MITM	Man-In-The-Middle
mmW	Millimeter Wave
MSCC	Multiple Sensor Consistency Check
NHTSA	The National Highway Traffic Safety Administration
OBM	On-Board Microcontroller
OEMs	Original Equipment Manufacturers
OTA	Over-The-Air
PKI	Public Key Infrastructure
PoS	Proof of Stake
PoW	Proof of Work
PSA	Physical Shift Authentication
PUF	Physically Unclonable Functions
PyCRA	Physical Challenge-Response Authentication System
Radar	Radio Detection and Ranging
RAIM	Receiver Autonomous Integrity Monitoring
RSUs	Road-Side Units
SAE	Society of Automotive Engineers
SDVN	Software Defined Vehicular Network
STCR	Spatio -Temporal Challenge-Response
SVM	Support Vector Machine
TLS	Transport Layer Security
TPMS	Tire Pressure Monitoring System
UAS	Unmanned Aerial System
VANETs	Vehicular Ad Hoc Networks
V2I	Vehicle-To-Infrastructure
V2V	Vehicle-To-Vehicle
V2X	Vehicle-To-Everything

compliance and standards requirements in the automotive sector. Organizations such as International Organization for Standardization (ISO), SAE, European Telecommunications Standards Institute (ETSI), International Electrotechnical Commission (IEC), etc., can consider incorporating the security countermeasures listed in this paper to the standards in Table V.

Though the standards and recommendations surveyed provide security baselines for functional safety, connected vehicles, and ITS communications, etc., the countermeasures in this paper address the most fundamental means by which an attacker can gain access to an autonomous vehicle, namely through its multi-faceted sensors. The intention is to prove that these countermeasures can be used in tandem with existing and on-going development standards to provide a comprehensive, defense-in-depth solution to address the current threat landscape.

VI. CONCLUSION

The contribution of this paper is to offer a timely review of potential cyber-attacks in autonomous vehicles. Specifically, the article discusses how malicious attackers in the sensing layer can exploit a modern car. Several cybersecurity threats are investigated under vehicle dynamics and environment sensors with their countermeasures. The authors see a transformative automotive industry that will soon adopt disruptive technologies (e.g., real-time machine learning, deep learning, advanced edge/fog computing, encryption, and blockchain) by integrating vehicular data from sensors in IoT platforms to advance the security and safety of vehicular networks.

APPENDIX

See Table VI.

REFERENCES

[1] NHTSA. (2018). *Automated Vehicles for Safety*. [Online]. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

[2] (2020). *Waypoint—The official Waymo Blog*. [Online]. Available: https://blog.waymo.com/

[3] (2020). *Tesla Autopilot AI*. [Online]. Available: https://www.tesla.com/autopilotAI

[4] (2020). *Cruise*. [Online]. Available: https://medium.com/cruise

[5] (2020). *Aptiv—CTO Blog*. [Online]. Available: https://www.aptiv.com/newsroom/cto-blog/253985928

[6] (Feb. 2019). *Self-Driving Cars Take the Wheel*. MIT Technology Review. [Online]. Available: https://www.technologyreview.com/2019/02/15/137381/self-driving-cars-ta%ke-the-wheel/

[7] S. International and Synopsys, "Securing the modern vehicle: A study of automotive industry cybersecurity practices," Ponemon Inst., Traverse City, MI, USA, Tech. Rep., 2019.

[8] S. International, "J3016B: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," SAE Int., Warrendale, PA, USA, Tech. Rep. J3016B, 2018. [Online]. Available: https://www.sae.org/standards/content/j3016 201806/

[9] A. Rastogi and K. Nygard, "Threats and alert analytics in autonomous vehicles," in *Proc. 35th Int. Conf.*, vol. 69, 2020, pp. 48–59.

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

[11] (2019). *Experimental Security Research of Tesla Autopilot*. [Online]. Available: https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Exp%erimental-Security-Research-of-Tesla-Autopilot/

[12] K. Eykholt *et al.*, "Robust physical-world attacks on deep learning visual classification," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2018, pp. 1625–1634.

[13] A. Lopez, A. V. Malawade, M. A. Al Faruque, S. Boddupalli, and S. Ray, "Security of emergent automotive systems: A tutorial introduction and perspectives on practice," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 36, no. 6, pp. 10–38, Dec. 2019.

[14] S. Plosz and P. Varga, "Security and safety risk analysis of vision guided autonomous vehicles," in *Proc. IEEE Ind. Cyber-Phys. Syst. (ICPS)*, May 2018, pp. 193–198.

[15] R. Sobers, "60 must-know cybersecurity statistics for 2019," *Varonis*, vol. 17, no. 60, p. 2019, Apr. 2019. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics

[16] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.

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

[18] C. Labrado and H. Thapliyal, "Hardware security primitives for vehicles," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 99–103, Nov. 2019.

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

[20] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100214.

[21] 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.

[22] J. Petit, M. Feiri, and F. Kargl, "Revisiting attacker model for smart vehicles," in *Proc. IEEE 6th Int. Symp. Wireless Veh. Commun. (WiVeC)*, Sep. 2014, pp. 1–5.

[23] J.-P. Monteuuis, J. Zhang, S. Mafrica, A. Servel, and J. Petit, "Attacker model for connected and automated vehicles," in *Proc. ACM Comput. Sci. Cars Symp.*, Sep. 2018, pp. 1–9.

[24] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Cryptographic Hardware and Embedded Systems*. New York, NY, USA: Springer, 2013, pp. 55–72. [Online]. Available: http://www.cyphylab.ee.ucla.eduhttp//www.nesl.ee.ucla.edu

[25] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications," in *Cryptographic Hardware and Embedded Systems—CHES*. New York, NY, USA: Springer, 2017, pp. 445–467.

[26] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," in *Defcon*, vol. 24, no. 8, p. 109, 2016.

[27] 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.

[28] I. Rouf *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. USENIX Secur. 19th USENIX Conf. Secur.*, 2010, pp. 1–16.

[29] B. G. Stotelaar, "Practical cyber-attacks on autonomous vehicles," M.S. thesis, Univ. Twente, Enschede, The Netherlands, May 2015.

[30] J. Petit, S. Bas, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," in *Black Hat Eur.*, vol. 11, p. 2015, Nov. 2015.

[31] 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. WOOT 10th USENIX Workshop Offensive Technol.*, 2016, pp. 1–11.

[32] Y. Son *et al.*, "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proc. 24th USENIX Secur. Symp.*, vol. 2015, pp. 881–896. [Online]. Available: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/p%resentation/son

[33] I. Giechaskiel and K. Rasmussen, "Taxonomy and challenges of out-of-band signal injection attacks and defenses," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 645–670, 1st Quart., 2020, doi: 10.1109/COMST.2019.2952858.

[34] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 1545–1562.

[35] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 3–18.

[36] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Secur. Symp. (USENIX Secur.)*, vol. 4, 2011, pp. 447–462.

[37] W. J. Fleming, "New automotive sensors—A review," *IEEE Sensors J.*, vol. 8, no. 11, pp. 1900–1921, Nov. 2008.

[38] (2017). *About the Conference*. [Online]. Available: http://www.automotivesensors2017.com

[39] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a mobile sensor," *Procedia Comput. Sci.*, vol. 34, pp. 286–295, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914008801

[40] F. Niewels, S. Knoop, R. Jordan, and T. Michalke, "In-vehicle sensors," in *Encyclopedia of Automotive Engineering*. Hoboken, NJ, USA: Wiley, 2014, pp. 1–27.

[41] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2nd Quart., 2006.

[42] D. Suo and S. E. Sarma, "A test-driven approach for security designs of automated vehicles," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2019, pp. 26–32.

[43] S. Nashimoto, D. Suzuki, T. Sugawara, and K. Sakiyama, "Sensor CON-fusion: Defeating Kalman filter in signal injection attack," in *Proc. Asia Conf. Comput. Commun. Secur. ASIACCS*, 2018, pp. 511–524, doi: 10.1145/3196494.3196506.

[44] E. Some, G. Gondwe, and E. W. Rowe, "Cybersecurity and driverless cars: In search for a normative way of safety," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Oct. 2019, pp. 352–357.

[45] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Attack resilience and recovery using physical challenge response authentication for active sensors under integrity attacks," 2016, *arXiv:1605.02062*. [Online]. Available: http://arxiv.org/abs/1605.02062

[46] M. Jo *et al.*, "Adaptive transient fault model for sensor attack detection," in *Proc. IEEE 4th Int. Conf. Cyber-Physical Syst., Netw., Appl. (CPSNA)*, Oct. 2016, pp. 59–65.

[47] J. Shin, Y. Baek, Y. Eun, and S. H. Son, "Intelligent sensor attack detection and identification for automotive cyber-physical systems," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov. 2017, pp. 1–8.

[48] J. Edwards, A. Kashani, and G. Iyer, "Evaluation of software vulnerabilities in vehicle electronic control units," in *Proc. IEEE Cybersecur. Develop. (SecDev)*, Sep. 2017, pp. 83–84.

[49] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[50] R. Matsumura, T. Sugawara, and K. Sakiyama, "A secure LiDAR with AES-based side-channel fingerprinting," in *Proc. 6th Int. Symp. Comput. Netw. Workshops (CANDARW)*, Nov. 2018, pp. 479–482.

[51] 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.

[52] G. Lu, D. Zeng, and B. Tang, "Anti-jamming filtering for DRFM repeat jammer based on stretch processing," in *Proc. 2nd Int. Conf. Signal Process. Syst.*, Jul. 2010, pp. 1–78.

[53] R. G. Dutta, F. Yu, T. Zhang, Y. Hu, and Y. Jin, "Security for safety: A path toward building trusted autonomous vehicles," in *Proc. Int. Conf. Comput.-Aided Design*, Nov. 2018, pp. 1–6.

[54] P. Kapoor, A. Vora, and K.-D. Kang, "Detecting and mitigating spoofing attack against an automotive radar," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.

[55] R. A. Raja Mahmood and A. I. Khan, "A survey on detecting black hole attack in AODV-based mobile ad hoc networks," in *Proc. Int. Symp. High Capacity Opt. Netw. Enabling Technol.*, Nov. 2007, pp. 1–6. [Online]. Available: https://www.researchgate.net/publication/4362772

[56] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "PyCRA: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. CCS*, 2015, pp. 1004–1015, doi: 10.1145/2810103.2813679.

[57] D. P. F. Moller, I. A. Jehle, and R. E. Haas, "Challenges for vehicular cybersecurity," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, May 2018, pp. 0428–0433.

[58] X. Shao, C. Dong, and L. Dong, "Research on detection and evaluation technology of cybersecurity in intelligent and connected vehicle," in *Proc. Int. Conf. Artif. Intell. Adv. Manuf. (AIAM)*, Oct. 2019, pp. 413–416.

[59] Y. Zhang, P. Shi, C. Dong, Y. Liu, X. Shao, and C. Ma, "Test and evaluation system for automotive cybersecurity," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE)*, Oct. 2018, pp. 201–207.

[60] D. K. Kilcoyne, S. Bendelac, J. M. Ernst, and A. J. Michaels, "Tire pressure monitoring system encryption to improve vehicular security," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, Nov. 2016, pp. 1219–1224.

[61] A. Kolodgie *et al.*, "Enhanced TPMS security through acceleration timed transmissions," in *Proc. MILCOM IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2017, pp. 35–39.

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

[63] Q. He, X. Meng, and R. Qu, "Survey on cyber security of CAV," in *Proc. Forum Cooperat. Positioning Service (CPGPS)*, May 2017, pp. 351–354.

[64] M. Harris. (2015). *Researcher Hacks Self-Driving Car Sensors*. [Online]. Available: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/r%esearcher-hacks-selfdriving-car-sensors

[65] Y. Takefuji, "Connected vehicle security vulnerabilities [commentary]," *IEEE Technol. Soc. Mag.*, vol. 37, no. 1, pp. 15–18, Mar. 2018.

[66] A. Rangesh and M. M. Trivedi, "No blind spots: Full-surround multi-object tracking for autonomous vehicles using cameras and LiDARs," *IEEE Trans. Intell. Vehicles*, vol. 4, no. 4, pp. 588–599, Dec. 2019.

[67] 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.

[68] S. Narain, A. Ranganathan, and G. Noubir, "Security of GPS/INS based on-road location tracking systems," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 587–601.

[69] 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.

[70] V. Hoa La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. Ad Hoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, Apr. 2014.

[71] A. K. Jadoon, L. Wang, T. Li, and M. A. Zia, "Lightweight cryptographic techniques for automotive cybersecurity," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–15, Jun. 2018.

[72] S. Khanafseh, N. Roshan, S. Langel, F.-C. Chan, M. Joerger, and B. Pervan, "GPS spoofing detection using RAIM with INS coupling," in *Proc. IEEE/ION Position, Location Navigat. Symp. PLANS*, May 2014, pp. 1232–1239.

[73] G. De La Torre, P. Rad, and K.-K.-R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, vol. 108, pp. 1092–1111, Jul. 2020.

[74] Y. Liu, S. Li, Q. Fu, and Z. Liu, "Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system," *Sensors*, vol. 18, no. 5, p. 1433, May 2018.

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

[76] J. Shin, Y. Baek, J. Lee, and S. Lee, "Cyber-physical attack detection and recovery based on RNN in automotive brake systems," *Appl. Sci.*, vol. 9, no. 1, p. 82, Dec. 2018.

[77] M.-J. Kang and J.-W. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in *Proc. IEEE 83rd Veh. Technol. Conf. (VTC Spring)*, May 2016, pp. 1–5.

[78] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198.

[79] W. Niu, X. Zhang, X. Du, T. Hu, X. Xie, and N. Guizani, "Detecting malware on X86-based IoT devices in autonomous driving," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 80–87, Aug. 2019.

[80] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.

[81] Z. Khan, M. Chowdhury, M. Islam, C.-Y. Huang, and M. Rahman, "Long short-term memory neural networks for false information attack detection in software-defined in-vehicle network," *IEEE Trans. Veh. Technol.*, 2019.

[82] I. Yaqoob, L. U. Khan, S. A. Kazmi, M. Imran, N. Guizani, and C. S. Hong, "Autonomous driving cars in smart cities: Recent advances, requirements, and challenges," *IEEE Netw.*, 2019.

[83] C. Wasner and J. Traxler, "AI and automotive safety," *ATZelectron. Worldwide*, vol. 14, no. 11, pp. 50–53, Nov. 2019.

[84] C. R. Banbury *et al.*, "Benchmarking TinyML systems: Challenges and direction," 2020, *arXiv:2003.04821*. [Online]. Available: http://arxiv.org/abs/2003.04821

[85] R. A. Michelin *et al.*, "SpeedyChain: A framework for decoupling data from blockchain for smart cities," in *Proc. 15th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, Nov. 2018, pp. 145–154.

[86] M. S. U. Alam, S. Iqbal, M. Zulkernine, and C. Liem, "Securing vehicle ECU communications and stored data," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[87] C. Qiu, F. R. Yu, F. Xu, H. Yao, and C. Zhao, "Blockchain-based distributed software-defined vehicular networks via deep Q-learning," in *Proc. 8th ACM Symp. Design Anal. Intell. Veh. Netw. Appl. DIVANet*, 2018, pp. 8–14.

[88] S. Mitra, S. Bose, S. S. Gupta, and A. Chattopadhyay, "Secure and tamper-resilient distributed ledger for data aggregation in autonomous vehicles," in *Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS)*, Oct. 2018, pp. 548–551.

[89] H. N. Nguyen, S. Tavakoli, S. A. Shaikh, and O. Maynard, "Developing a QRNG ECU for automotive security: Experience of testing in the real-world," in *Proc. IEEE Int. Conf. Softw. Test., Verification Validation Workshops (ICSTW)*, Apr. 2019, pp. 61–68.

[90] W. Wang and M. Stöttinger, "Post-quantum secure architectures for automotive hardware secure modules," vol. 2020, Jan. 2020.

[91] T. Fritzmann, J. Vith, and J. Sepúlveda, "Post-quantum key exchange mechanism for safety critical systems," Tech. Rep., 2019.

[92] N. Ravi and S. M. Shalinie, "Semi-supervised learning based security to detect and mitigate intrusions in IoT network," *IEEE Internet Things J.*, early access, May 8, 2020, doi: 10.1109/JIOT.2020.2993410.

[93] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.

[94] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," *J. Parallel Distrib. Comput.*, vol. 119, pp. 18–26, Sep. 2018.

[95] W. Xue *et al.*, "Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things," *IEEE Trans. Mobile Comput.*, early access, May 6, 2020, doi: 10.1109/TMC.2020.2992737.

[96] P. K. Agarwal and C. T. Howell, "Addressing privacy and security issues in the connected car," *IndustryWeek*, Feb. 2017. [Online]. Available: https://www.industryweek.com/emerging-technologies/addressing-privacy-and-security-issues-connected-car

[97] IEEE, "Artificial intelligence and machine learning applied to cybersecurity," IEEE, Washington, DC, USA, Tech. Rep., Oct. 2017.

[98] P. Nakkiran, G. Kaplun, and I. Sutskever. (2019). *Deep Double Descent*. [Online]. Available: https://openai.com/blog/deep-double-descent/

[99] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, "A survey of autonomous driving: Common practices and emerging technologies," *IEEE Access*, vol. 8, pp. 58443–58469, 2020.

[100] Y. Wang, W.-L. Chao, D. Garg, B. Hariharan, M. Campbell, and K. Q. Weinberger, "Pseudo-LiDAR from visual depth estimation: Bridging the gap in 3D object detection for autonomous driving," 2018, *arXiv:1812.07179*. [Online]. Available: http://arxiv.org/abs/1812.07179

[101] L. Burrows. (Jun. 2019). *Setting the Standard for Machine Learning*. [Online]. Available: https://phys.org/pdf480675475.pdf

[102] P. Sharma, D. Austin, and H. Liu, "Attacks on machine learning: Adversarial examples in connected and autonomous vehicles," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Nov. 2019, pp. 1–7.

[103] A. Gantait, J. Patra, and A. Mukherjee, "Integrate device data with smart contracts in IBM blockchain," *IBM Developer*, Jun. 2017. [Online]. Available: https://developer.ibm.com/articles/cl-blockchain-for-cognitive-iot-apps-trs/

[104] D. C. P. G. Saranti and S. Karatzas, "Autonomous vehicles and blockchain technology are shaping the future of transportation," in *Proc. Conf. Sustain. Urban Mobility*, 2018, pp. 797–803.

[105] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[106] L. Li *et al.*, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[107] M. Wagner and B. Mcmillin, "Cyber-physical transactions: A method for securing VANETs with blockchains," in *Proc. IEEE 23rd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Dec. 2018, pp. 64–73.

[108] M. Wazid, A. K. Das, S. Shetty, and M. Jo, "A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things," *IEEE Access*, vol. 8, pp. 88700–88716, 2020.

[109] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in VANET," in *Proc. IEEE 3rd Int. Conf. Comput., Commun. Secur. (ICCCS)*, Oct. 2018, pp. 161–166.

[110] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95021–95033, 2019.

[111] Nyamtiga, Sicato, Rathore, Sung, and Park, "Blockchain-based secure storage management with edge computing for IoT," *Electronics*, vol. 8, no. 8, p. 828, Jul. 2019.

[112] M. Andoni *et al.*, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[113] S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K.-R. Choo, and A. Y. Zomaya, "Blockchain for smart communities: Applications, challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 144, pp. 13–48, Oct. 2019.

[114] K. Sharma and D. Jain, "Consensus algorithms in blockchain technology: A survey," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2019, pp. 1–7.

[115] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1432–1465, 2nd Quart., 2020.

[116] S. J. Alsunaidi and F. A. Alhaidari, "A survey of consensus algorithms for blockchain technology," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Apr. 2019, pp. 1–6.

[117] G. Bashar, G. Hill, S. Singha, P. Marella, G. G. Dagher, and J. Xiao, "Contextualizing consensus protocols in blockchain: A short survey," in *Proc. 1st IEEE Int. Conf. Trust, Privacy Secur. Intell. Syst. Appl. (TPS-ISA)*, Dec. 2019, pp. 190–195.

[118] E. Uhlemann, "Time for autonomous vehicles to connect [connected vehicles]," *IEEE Veh. Technol. Mag.*, vol. 13, no. 3, pp. 10–13, Sep. 2018.

[119] *Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)*, Standard ETSI TR 102 893, International Standard, European Telecommunications Standards Institute, Sophia Antipolis Cedex, France, Mar. 2017.

[120] *Intelligent Transport Systems (ITS); Security; Its Communications Security Architecture And Security Management*, Standard ETSI TS 102 940, International Standard, European Telecommunications Standards Institute, Sophia Antipolis Cedex, France, Apr. 2018.

[121] *IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages*, Standard 1609.2-2016, International Standard, International Organization for Standardization, NJ, USA, Jan. 2016.

[122] *Functional Safety*, Standard ISO 26262, International Standard, International Electrotechnical Commission, Geneva, Switzerland, Apr. 2010.

[123] *Electrical and Electronic Components and General System Aspects*, Standard ISO/TC 22/SC 32, International Standard, International Organization for Standardization, Tokyo, Japan, 2014.

[124] *Road Vehicles—Functional Safety*, Standard ISO 26262-1:2018, International Standard, International Organization for Standardization, NJ, USA, Dec. 2018.

[125] *Road Vehicles—Cybersecurity Engineering*, Standard ISO/SAE DIS 21434, International Standard, International Organization for Standardization, NJ, USA, 2020.

[126] R. E. Haas and D. P. F. Moller, "Automotive connectivity, cyber attack scenarios and automotive cyber security," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2017, pp. 635–639.

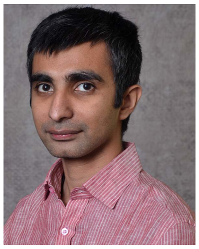
[127] M. Scalas and G. Giacinto, "Automotive cybersecurity: Foundations for next-generation vehicles," in *Proc. 2nd Int. Conf. New Trends Comput. Sci. (ICTCS)*, Oct. 2019, pp. 1–6.

Zeinab El-Rewini received the B.S. degree in computer science and the B.A. degree in political science from the University of North Dakota (UND), USA, in 2018. She was a Product Engineering Intern at John Deere Electronic Solutions, where she joined the Software Engineering Tools and Infrastructure (SETI) Team in creating testing software for electronic control units used within John Deere Machinery. In the Fall of 2018, she was an Undergraduate Research Scholar with the Data, Energy, Cyber and Systems (DECS) Laboratory, UND.

Karthikeyan Sadatsharan received the bachelor's degree in electronics and communication engineering from Anna University, India, and the master's degree in telecommunications engineering from the University of Texas at Dallas, USA. He currently works as an Antenna Test Engineer with Honda R&D Americas, OH, USA. He previously worked as an RF Systems Engineer at Ford Motor Company, Detroit, USA. His research interests include RF and microwave design and communication systems design for autonomous vehicles technology.

Niroop Sugunaraj received the B.E. degree (computer science) in engineering from the University of Wollongong in Dubai (UOWD), Dubai, United Arab Emirates, in 2018. He is currently pursuing the master's degree in electrical engineering with the College of Engineering and Mines (CEM), UND. He was a Design and Development Engineering Intern at Lockheed Martin, Abu Dhabi, where he collaborated with engineers in USA. He is also a Researcher at the Data, Energy, Cyber and Systems (DECS) Laboratory, UND.

Daisy Flora Selvaraj is currently a Research Engineer at the Energy and Environmental Research Center (EERC), University of North Dakota (UND), Grand Forks, ND, USA. Her research interests include grid integration of renewable energy systems and batteries, smartgrid, and condition monitoring of power apparatus.



Siby Jose Plathottam is a Postdoctoral Appointee with the Energy Systems Division, Argonne National Laboratory. His research interests include distributed energy resource modeling, control system design, and utilizing deep learning in power system applications.

Prakash Ranganathan (Senior Member, IEEE) is currently an Assistant Professor with the School of Electrical Engineering and Computer Sciences (SEECS) and the Director of the Data, Energy, Cyber and Systems (DECS) Laboratory, University of North Dakota (UND). He also plays a leadership role in facilitating research initiatives on the Big Data and Cybersecurity research thrusts for the Research Institute for Autonomous Systems (RIAS), a center to advance research on autonomous systems at the UND. His research interests include machine learning, operations research, smart grid, data mining, and cybersecurity.