Received 3 March 2022; revised 1 April 2022; accepted 16 April 2022. Date of publication 25 April 2022; date of current version 10 May 2022.

Digital Object Identifier 10.1109/OJCOMS.2022.3169500

Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey

MUHAMMAD HATABA[1,2] (Member, IEEE), AHMED SHERIF[1] (Senior Member, IEEE), MOHAMED MAHMOUD[3] (Senior Member, IEEE), MOHAMED ABDALLAH[4] (Senior Member, IEEE), AND WALEED ALASMARY[5] (Senior Member, IEEE)

[1]School of Computing Sciences and Computer Engineering, University of Southern Mississippi, Hattiesburg, MS 39401, USA

[2]Computer and Systems Department, National Telecommunications Institute, Cairo, Egypt

[3]Department of Electrical and Computer Engineering, Tennessee Tech University, Cookeville, TN 38505, USA

[4]Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

[5]Department of Computer Engineering, Umm Al-Qura University, Mecca 24382, Saudi Arabia

CORRESPONDING AUTHOR: A. SHERIF (e-mail: ahmed.sherif@usm.edu)

ABSTRACT Artificial Intelligence (AI) is changing every technology we are used to deal with. Autonomy has long been a sought-after goal in vehicles, and now more than ever we are very close to that goal. Big auto manufacturers as well are investing billions of dollars to produce Autonomous Vehicles (AVs). This new technology has the potential to provide more safety for passengers, less crowded roads, congestion alleviation, optimized traffic, fuel-saving, less pollution as well as enhanced travel experience among other benefits. But this new paradigm shift comes with newly introduced privacy issues and security concerns. Vehicles before were dumb mechanical devices, now they are becoming smart, computerized, and connected. They collect huge troves of information, which needs to be protected from breaches. In this work, we investigate security challenges and privacy concerns in AVs. We examine different attacks launched in a layer-based approach. We conceptualize the architecture of AVs in a four-layered model. Then, we survey security and privacy attacks and some of the most promising countermeasures to tackle them. Our goal is to shed light on the open research challenges in the area of AVs as well as offer directions for future research.

INDEX TERMS Autonomous vehicles, communication system security, information system security, data privacy.

I. INTRODUCTION

THE INDUSTRIAL revolution is still evolving, and now we are in the most significant shift of all, eliminating the need for the human factor. Artificial intelligence, machine learning, and intelligent robotics can already replace humans in various fields, such as manufacturing, medicine, economics, education, and public safety. One key field, which long suffered from human mistakes, is transportation. Hundreds of thousands of people die in car accidents every year [1]. The total adoption of autonomous driving systems would significantly decrease human errors and allow for more efficiency in various aspects, such as better fuel utilization, lower accident rates, and of course, passenger welfare while offering a pleasant entertainment-rich experience.

Unfortunately, regardless of the expected benefits of AVs, these systems are still facing plenty of security issues and privacy concerns [2]. Vehicles, which used to be all-in-all mechanical systems, are now inheriting computer systems problems that are susceptible to a wide range of unexpected attacks. This happens more often when these systems are connected via communication networks, thereby opening the system to the outside world or even malicious insiders in the network. An autonomous driving system would not have

thrived without the need for networking. AVs need to communicate with each other and with the Internet to navigate their way, download firmware updates, participate in traffic management systems, etc. [3], by getting updated maps and information about busy roads and traffic congestion. Also, the autonomous driving system needs a continuous connection to the car manufacturer's cloud, which monitors the vehicle's condition and provides aid if needed [4].

Relying solely on the vehicle's sensors, such as proximity sensors, cameras, and light detectors, is not enough for AVs' safe operation. That is because these sensors may have physical limitations, which may result in making erroneous decisions [5]. That is why vehicles need to communicate with each other to make up for these deficiencies by exchanging information on road and traffic conditions, thereby improving the navigation of vehicles. Moreover, serious accidents can be mitigated if vehicles communicate continuously, thereby avoiding collisions and improving road safety [6].

Additionally, modern vehicles allow users to connect their smartphone, other portable, or more recently wearable devices via various wired (AUX, USB, etc.) and wireless interfaces (WIFI, Bluetooth, etc.) in a seamless integration [7]. This sort of connection allows for sharing data between the vehicle and the mobile device for playing music, answering phone calls, checking social media notifications, and surfing the Web [8]. These devices may make the car system susceptible to new attacks and vulnerabilities since they are inherently prone to hacking and malware programs [9].

Security attacks are an enormous threat to autonomous driving systems. Successful cyberattacks may cause system failure, which may lead to accidents and thus losing human lives. Moreover, malicious hackers can deliberately target a particular vehicle and disrupt its normal operation to steal it or even harm others or cause any damage. In addition, privacy is a major concern in AVs. The continuous communication between the vehicle and its surroundings puts the user's private data at risk. Potential threats include information leakage, identity theft, tracking, and stalking. Users may not trust technology providers because they may collect sensitive information and sell it to interested parties. Imagine an intelligent car equipped with cameras and a microphone, and a variety of sensors that can be used to harness troves of data on the car's passengers [10].

In this paper, we present a survey on security and privacy issues in autonomous driving systems. We classify these issues from a layer-based perspective inspired by the TCP/IP network model [11], which was based on the OSI reference model of computer networks [12]. Figure 1 shows the layered structure of the AVs system that we are focusing on; application layer, operating system layer, network layer, and physical layer. We are not concerned with software or hardware faults arising within the system itself. Instead, we focus on the dangers of opening the system to its surroundings and the outside world via various wired or wireless communication channels.

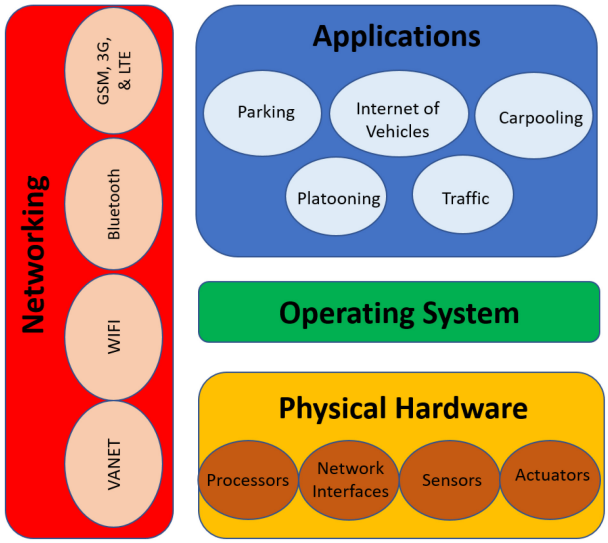

FIGURE 1. The expanded layered structure of autonomous vehicles system.

The remainder of this paper is organized as follows. Section II shows an overview of the literature related to a variety of application layer programs that are quite popular in the realm of AVs, their major security and privacy challenges. The vulnerabilities of the AV operating system layer are investigated in Section III. Section IV focuses on the security issues regarding the network layer. In Section V we discuss the hardware attacks on AVs. Additionally, in Section VI we show some related works that surveyed AV security and privacy issues. Finally, in Section VII we conclude the paper and suggest directions for future work.

II. APPLICATION LAYER SECURITY

Autonomous driving systems allowed for a new generation of applications, some of which may have existed before, but with the vehicles being able to drive themselves, researchers had to revolutionize these applications to make use of the new possibilities. And with the new possibilities comes new security risks that must be addressed before the total adoption of these applications and creating room for much more. Some example application includes; but not limited to, carpooling, automated valet parking, automated electrical charging (since most modern AVs will be electrical), sensor data gathering, forensics, platoon stability, safe navigation and crash prevention applications; video upload (e.g., an accident scene, Pic-on-wheels, remote drive,. . . , etc.), news, entertainment, location-relevant info download, driver behavior study, traffic crowdsource, mitigating congestions/pollution by efficient routing and intelligent transport [17].

Here we shed some light on primary application areas and an overview of the work being done to secure them.

1) TRAFFIC FLOW OPTIMIZATION

In traffic flow optimization, traffic is directed through a road network in order to minimize travel times, eliminate traffic

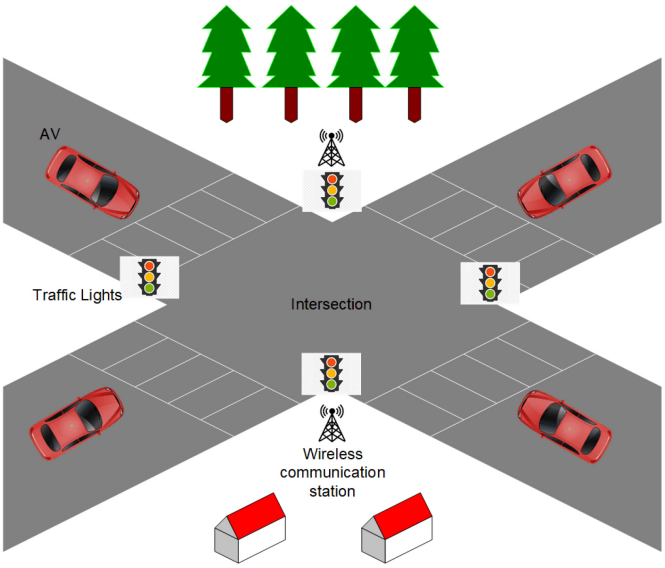

FIGURE 2. A typical traffic management system would control intersections, traffic lights and ramp meters among other things.

congestion, and maximize overall road infrastructure utilization. Currently, new approaches seek to influence vehicles through the adaptation of traffic signal schedules [18], [19] and digital signage, as illustrated in Figure 2. When AVs are present, the method can take an entirely new form.

Many researchers tried to simulate and study the traffic management systems, such as [20], [21]. Some researchers focused on ramp metering as in [22], while others concentrated on intersection management on a larger scale such as [23] and [24]. That said, besides the AV traffic management algorithm itself, which is sometimes quite complicated, there are side problems that need to be handled [25] such as the coexistence of AV with human-driven cars, pedestrians, motorcyclists, etc.; dealing with complicated situations such as severe weather conditions or natural accidents, advanced architecture support. There are also data handling and communication problems.

Here we focus on traffic messages being communicated by the car. These are vulnerable to a variety of network-level security attacks that we will further investigate in Section IV. Moreover, stakeholders' privacy is of primary concern, and there has been a considerable effort to protect it.

In [13], the authors proposed a model based on data quality evaluation metrics to augment trust and reputation. Their proposed model can detect agents that supply incorrect or fraudulent data; thereby, they can be removed, and hence the overall system accuracy can be enhanced.

Another piece of work that we studied is the work in [14], where the authors proposed a scheme to protect the privacy of vehicles sharing their routes to a traffic-flow optimization. Knowing that these systems need only to learn the number of vehicles traveling in the same road segment, anticipating possible congestion situations, the authors developed a segment-based route reporting system that sends data encrypted using homomorphic encryption to roadside units (RSUs). All segment data from different vehicles are then collected at RSUs. It computes the encryption of the number of anticipated cars occupying every road segment without knowing the actual routes of vehicles. Then, this information is shared with a traffic management center (TMC), that computes the decryption and extracts that same number while individual vehicles' routes are hidden for privacy preservation. After analyzing this information, the TMC can send directions to traveling cars about traffic conditions and congestion.

Another significant issue affecting traffic systems is Sybil attacks. In such a type of attack, individual attackers can imitate multiple vehicles that submit a bogus incident down the road. Generally, a traffic system requires information regarding events in order to notify vehicles of unanticipated road hazards and ensure safe driving. The authors of [15] presented a secure event-reporting mechanism to thwart Sybil attacks while maintaining users' privacy. The proposed scheme distributes a set of pseudonyms/keys to enable reporting of incidents without disclosing private vehicle information. Additionally, the authors proposed a method for identifying the vehicles that conduct Sybil attacks using their pool of pseudonyms. The proposed scheme classifies vehicles into groups, and the RSUs only know the group numbers of the vehicles, not their identities. If the pseudonyms keys were used to report an incident related to the same group, the RSUs would suspect a singular Sybil attack. In this situation, the RSUs transmit the messages to the department of motor vehicle (DMV). Sybil attacks are recognized when the DMV determines that the suspicious pseudonyms are associated with a particular vehicle. Even if numerous attackers collaborate, the RSU will detect it when it compares the beacon packet signals from the vehicles to the reported events.

More interestingly, the authors in [16] went as far as using unmanned aerial vehicles (UAV) to assist with road monitoring. They proposed a so-called security situational aware intelligent traffic monitoring, which can re-route the traffic, offer guidance instructions for shortest routes with the help of a traffic management security control center. They combine information from graph theory representation of the road map with sensory networks. UAVs' usage enables real time and rapid response to different security cases, since it shouldn't encounter any hindrances to wireless communications in comparison with traditional traffic monitoring systems.

Although the discussed techniques may be promising, we think that in the future, some of these techniques can be integrated together into a more comprehensive intelligent vehicular transportation system, which is trained against different security attack scenarios and protect the stakeholders' data. Table 1 summarizes these findings and our critique of them.

TABLE 1. Security & privacy attacks on traffic flow optimization applications.

Ref. No.	Threat	Proposed Method	Critique
[13]	Data integrity	Data quality evaluation metrics	Susceptible to Sybil, man-in-the-middle, and repudiation attacks.
[14]	Privacy of vehicle routes	Segment-based route reporting and homomorphic encryption	Incurs performance cost in terms of computation overhead, communication cost and power consumption.
[15]	Sybil attacks	Pseudonyms/keys and vehicle grouping with RSUs	Management of groups may become an overhead. Also, there is considerable communication overhead.
[16]	Data Integrity	Road Monitoring using UAVs	Requires huge set up cost, and maintenance of the UAVs. Also, they become honeypot for attacks.

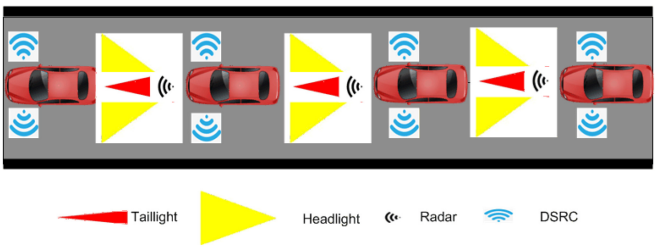

FIGURE 3. An Autonomous vehicles platoon and the various sensors they use.

2) PLATOONING

AVs platoon, as depicted in Figure 3, is an advancement of autonomous conduct in which AVs are assembled into clusters of cars in close range and communicate wirelessly [26]. Cooperative adaptive cruise control (CACC) can be thought of as an improved version of adaptive cruise control (ACC) that is used in this group of vehicles [30]. This system enables vehicles to keep a proper distance from one another and make cooperative navigation decisions. Since the vehicles in a platoon work together to plan ahead and drive closer together, the platoon improves traffic flow. In addition, the ability to respond to events more quickly than drivers improves transportation safety. Moreover, lessening the amount of time spent accelerating and decelerating on the road helps save fuel and reduce emissions.

Most platoon members communicate via IEEE 802.11p, the most common vehicular RF technology. However, this technology has vulnerabilities that various malicious attackers can exploit. In applications that involve collaborative driving, an unexpected surfacing of a security threat may endanger the following: (i) the integrity of traffic flow messages on the AV network by submitting fake data that change the platoon organization and coordinated movements; and (ii) the stability of platoon applications by affecting communication capabilities in the AV network.

AVs in a platoon are more tightly coupled than ordinary cars, making them more vulnerable to attacks targeting their platoon system. In [31] the authors showed that a single malicious AV could destabilize an entire platoon and cause catastrophic events. This malicious car combines some changes to the gains of the control law with vehicle movements, thereby forcing the platoon to oscillate at a resonant frequency and violating the platoon string stability features, resulting in fatal accidents. In [32], the authors managed to mimic a high-speed collision induction attack by overtaking the platoon controller. They manipulated the DSRC to cause an expected behavior from a platoon member, thereby causing collisions. In [33] the authors showed that a malicious AV could introduce a precise effect on the mobility of vehicles in its vicinity, thereby raising the energy expenditure of neighbouring vehicles by 20% to 300%.

In [34], [35] the authors provided an in-depth study into the control laws of AV in a platoon. They showed that one malicious AV could introduce erroneous traffic messages that other vehicles can then amplify, causing traffic jams or accidents. They studied the conditions under which the attacker can disrupt the AV stream and the string stability and proved that such disruption will self-perpetuate as one of the vulnerabilities of relying on AV compared to human-driven cars unless additional inputs are provided.

By utilizing light's directivity and impermeability, visible light communication (VLC) can mitigate these vulnerabilities. On the other hand, using just VLC in a platoon might affect its safety due to VLC's sensitivity to environmental effects. SP-VLC [26] is a VLC and IEEE 802.11p based protocol for securing communications in platoons. This protocol ensures stability of platoons and security of their motions under different types of attacks such as jamming, channel overhearing and injection of data packets. They describe these maneuver attacks by defining various circumstances in which a malicious party sends a forged maneuver packet. SP-VLC contains techniques for establishing an encryption key, authentication of messages, communications over both VLC and IEEE 802.11p, detection of jamming attacks and response to switching to VLC-only transmission, and movement safety depending on both VLC and IEEE 802.11p. Additionally, they develop a simulation platform that incorporates a realistic vehicle mobility model, realistic VLC and IEEE 802.11p channel models, and platoon management for vehicles.

In [27], the authors investigate how to secure AV platooning when an unknown vehicle is attacked and bounded system uncertainties occur. A malicious attacker can arbitrarily modify the attacked vehicle's GPS position and speed measurements. In the beginning, two detectors were proposed to determine which car is being attacked based on relative measurements (camera or radar) and local information gathered from measurements of surrounding vehicles. They next create a local state observer for each vehicle based on the detectors' data by using a saturation method to

TABLE 2. Security & privacy attacks on platoon applications.

Ref. No.	Threat	Proposed Method	Critique
[26]	Jamming, channel overhearing and injection of data packets	SP-VLC	Attacker with enough knowledge about the switching scheme can exploit VLC vulnerabilities, if coupled with other attack vectors.
[27]	Unknown vehicle is attacked and bounded system uncertainties occur	Relative measurement and local state observer	Susceptible to collusion, the observer can be a honeypot for attacks.
[28]	Message falsification and spoofing attacks	Cooperative control technique	Voting algorithm can be exploited by colluding vehicles.
[29]	Attacks on Message authentication and security	VPKIbrID	Public key infrastructure and Attribute Based Encryption require large computation cost, communication overhead and power consumption.

the measurement innovation. Additionally, based on the observer's neighbor state estimates, a distributed controller is presented to establish vehicle speed consensus and maintain a stable desired distance between two neighboring vehicles. Under certain conditions, it was demonstrated that the observer's estimate error and the controller's platooning error are asymptotically upper-bounded.

In [28], the authors focus on several important forms of attacks which impact security of platoons. They examined Burst Transmission and DoS attacks, which affect the network layer. They also studied message falsification and spoofing attacks, that target the application layer. The paper proposed a new closed-loop collaborative control technique for strengthening autonomous platoon security. They also implemented their system in PLEXE [36] and analytically proved its claimed stability.

In [29] the authors studied the security of underlying vehicular network which supports platoon management protocol. The proposed model uses Public Key Infrastructure and Attribute Based Encryption with Identity Manager Hybrid (VPKIbrID). This robust encryption scheme would ensure message communication authentication and security. They simulated their system using various sizes of platoons and different modes of VPKIbrID propagating different numbers of multicast/broadcast messages.

As we can see from this investigation, platooning is a complex application that requires security precautions at several layers. The interactions between the AV, the Connectivity Control Unit (CCU) should be strongly authenticated and defined in a lightweight key management scheme. A secure design for a Dedicated Short Range Communications (DSRC) communication protocol robust to different attack types, including packet falsification, replay, jamming, membership falsification, and hijacking, is still needed. In Table 2 we summarize this discussion and our comments.

3) CARPOOLING

Carpooling or ride-sharing has emerged in the last decade. Carpooling is a system which requires different individuals having interchangeable journeys to ride together in one car at the same time, instead of having different cars [37]. By decreasing the quantity of cars on the roads, carpooling will lessen air pollution and traffic congestion. It can also share the cost of the trip between several people.

Companies like Uber and Lyft certainly revalorized the transportation industry and made a seismic shift in the employment market. In many countries now, and as a part-time job, many users utilize their vehicles as ride-hailing vessels through these apps, thereby significantly enhancing their income. On the other hand, from the passenger side, these apps allow for a much more convenient customer experience when dealing with an easy-to-use app, precisely calculated fare in advance, and an easy-to-use customer complaint and dispute facility through the same apps. Eliminating the driver from the whole equation is a perfect opportunity for every car owner who had been toying with the idea to use his car in carpooling. He no longer has to sacrifice time and effort to make some extra money. Service-providing companies may not worry anymore about customers having uncomfortable situations with drivers. We have to mention that some companies may opt to abandon this decentralized business model altogether and build their fleet of autonomous vehicles, but this may not be economically attractive as the first model.

The use of ride-sharing has risen considerably [41]. As of 2010, North America had at least 613 platforms for ride-sharing organizations primarily based on the Internet [42], [43], [44]. Additionally, many government programs have already been made to allow people to share trips. One such strategy is to make high occupancy vehicle (HOV) lanes. This requires a reserved lane to be used for cars with more than two passengers on board [45], [46]. Another tactic for promoting ride sharing is to include toll reductions, and refunds [47].

Figure 4 shows a typical architecture of an AV carpooling system. The organization of shared rides can be significantly improved by the use of Internet access, GPS systems and smartphones. Customer registration is expected to be done through a Web portal which manages shared trips, and afterwords submit a ridesharing offer to a Trip Organizing Server (TOS) via a car owner (operator) and wanting to share a trip with other customers (riders). This offer would provide details on the travel, such as the location, destination, time of the trip, and direction. Moreover, passengers requesting mutual transportation can first send requests for ridesharing with specific details to the TOS. Then, TOS compares offers from drivers with requests from riders, thus allocating each driver to one or more passengers. Nevertheless, the TOS

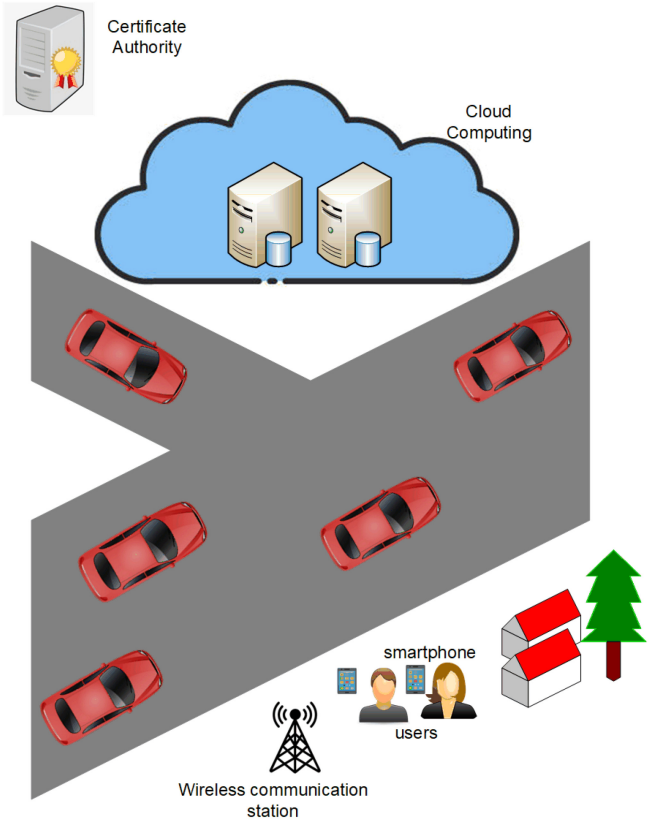

FIGURE 4. Architecture of an AV carpooling system.

is owned and managed by a private corporation that may gather information about the locations and behaviors of the customers and may launch user impersonation, forgery, and replay attacks.

But the catch is how to make the customer trust these indigent cars with his/her private data such as the locations they visit, their trips, their usage patterns, and use the service with a level of anonymity. On the other hand, car owners should trust that their cars will not be stolen, vandalized, or used in some malicious endeavors. The service provider should worry about both the car owner and the customer, and at the same time, protect itself from untrusted users who try to hack the system for their gain. Some users may report false locations to match certain passengers/cars or attract traffic to some area for malicious purposes.

Although most of the work on carpooling applications focused on human-driven cars, similar ideas can be applied to AVs. Here we investigate some of these ideas and discuss how they relate to AVs.

In particular, secure and privacy-preserving schemes for ride-sharing is now an essential need to flourish the usage of AVs [48], [49]. In [37], the authors proposed effective privacy-preserving ride-sharing management techniques for transferable and non-transferable ride-sharing systems. In a non-transferable ridesharing service (NRS), a trip organizing server (TOS) would execute matching over encrypted data to associate a single driver to each rider. Nevertheless, TOS utilizes trip data from the drivers in the transferable ridesharing service (TRS) to construct an encrypted directed graph for the management of carpooling. Preferences of the riders are used to determine the weights of the graph's edges. Nevertheless, TRS provides an attractive service that can expand ridesharing. At the same time, NRS offers a valuable and convenient service for the aged and disabled, who do not want to switch between multiple drivers.

One promising piece of work [38], entirely suited to this seemingly decentralized model, is the use of blockchain technology. The authors proposed to build a private blockchain ledger to store all carpooling records. They also proposed storing locations grid into a tree and achieving drop-off locations matching by a range query scheme. They also adopted a privatized proximity check to attain one-to-many proximity matching and expand it to effectively set up a secret communication key between a rider and a driver. In [39] the authors went into more details about users' privacy location tags, range queries, and anonymous authentication. But the difference here is that instead of using fog computing, they relied on a central cloud server. They were working under the assumption that this server might be honest-but-curios. That is why they suggested using blockchain technology to record all the hashes and trip records.

Additionally, the authors of [40] proposed B-Ride, a decentralized ride-sharing service built on public Blockchain. They examined a scenario in which fraudulent users could take advantage of the anonymity given by the public Blockchain to submit many bogus ride requests or offers while remaining uncommitted to any of them to secure a better deal or render the system unstable. As a result, the paper developed a time-locked deposit mechanism based on smart contracts and zero-knowledge set membership proof. The driver and the rider must demonstrate exemplary conduct by making deposits to the Blockchain. This will be considered when determining the fair in a pay-as-you-drive system based on the driver and rider's elapsed distance. Additionally, they implement a reputation model to assess drivers based on their prior behavior without involving third parties, allowing riders to choose drivers based on their history on the system.

In summary, the introduction of new prospects from AVs will bring forth a massive transition into carpooling applications. In this context, ongoing research efforts should address a situation where adversaries compromise the RSUs. Tamper-proof Blockchains are not enough since we need a mechanism to authenticate data feed from users in case of disputes [50]. Crowdsourcing mechanisms [51] can be integrated to be a witness in claims and proofs. Anonymous, yet secure payment mechanism for carpooling services is also an open area of research. Table 3 gives a summary of the literature discussed above and our thoughts of them.

4) PARKING

Parking is one of the most significant issues in many major cities worldwide. Due to the increase in population density

TABLE 3. Security & privacy attacks on carpooling applications.

Ref. No.	Threat	Proposed Method	Critique
[37]	Privacy of user and AV data	TOS executes matching over encrypted data	TOS is the central point of failure in the system, also, it doesn't account for collusion and double booking attacks.
[38]	Compromising privacy of user and AV data	Blockchain	Susceptible to fraudulent submissions. Also, the heave computation overhead.
[39]	Compromising Location privacy	Central cloud server, anonymous authentication	The central cloud is a honeypot for attacks. Also, there is more communication overhead and setup costs.
[40]	Compromising privacy of user and AV data	Blockchain and Time-locked deposit	The system is too complicated and difficult to be scalable.

and the number of cars in the streets, it is not always easy to find a spot to park your vehicle near your home, the place you work at, or even in front of the shop or the venue you are visiting. During special events and holidays, this could be a nightmare. That's why many cities built big parking lots in every neighborhood, but sometimes they may not be close to your desired destination. Moreover, in many cases, you may have to visit multiple places to find an empty spot, thereby losing more time, effort, fuel, and at the same time, causing unnecessary traffic load to the already crowded cities.

It is worth mentioning that big tech giants, which may not seem directly involved with car manufacturing, have numerous patents dealing with various aspects of parking in AVs. Such as [56] which is owned by IBM and provides an algorithm to optimize the delay in the parking process, which detects the last embarking passenger of the car and then initiates the parking process automatically. It deals with the steering system, transmission controls, and brakes to cause the vehicle to park in and out of parking spots from/into the roadway. On the other hand, car manufacturers are still developing ways to deal with physical control issues of parking systems. For example, in [57], Ford developed an electric braking system tailored for parking AVs. Also, in [58] Volkswagen developed a system for data processing for obtaining the operational state of AVs.

Having an AV park itself is an excellent idea, and it will save much-needed time and effort. But there must be coordination between the parking lots and the AV to guide through the process. Figure 5 depicts an example of an automated parking system for AVs. An efficient system would have an app that tells you where to find empty parking spots nearby the destination you want. Then your car would drop you off and go there to park itself. When you finish your business there, you will order the car to come to pick you up. All payment and handling fees would be automatically charged to your account in a seamless manner. Sounds perfect, but here is the catch. How do you trust that your car will not be stolen or vandalized. An inside attacker may thieve other parked AVs by launching attacks such as man-in-the-middle, forging, replay, and impersonation attacks. Theses attacks also can be launched remotely by an outside attacker. Their objective is to compromise the authentication between AVs and smartphones that control them, hence, he could start the motor and run away with the AV.

Another major problem is how you would trust that your location privacy will not be compromised. Here, the attacker

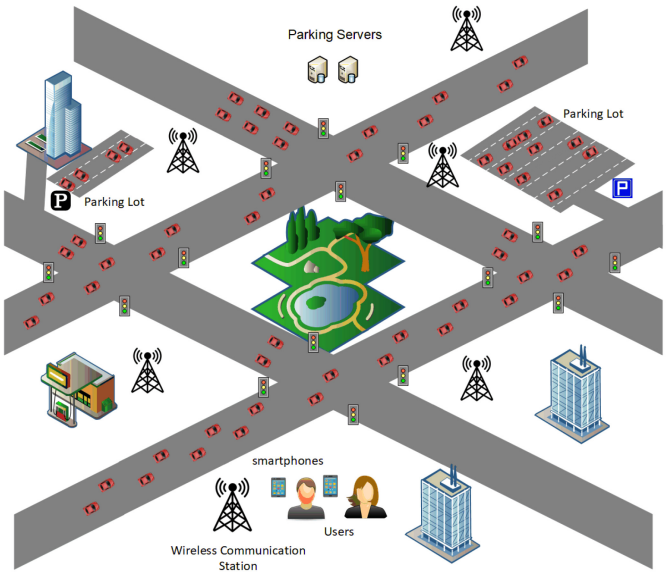

FIGURE 5. An example of an automated parking system for AVs.

may try to identify a specific user's location. Moreover, a nefarious attacker could cooperate with other adversaries and penetrate the system and automated parking computers to predict a victim user's location based on the position of AVs.

Additionally, an adversary may actually follow some particular AV and intercept every messages it receives and obtain access to the local server's and automated parking system server's secret keys. If the attacker is not capable of knowing the AV owner in advance, the attacker cannot compromise the user's location privacy. Another concern is slandering, in which an attacker may pretend that an honest user scratched his vehicle. The attacker could be a registered but malicious user who provides the judge with enough location information to classify an honest user as a scratching perpetrator. Another instance of defamation is when a legitimate but wicked user slanders the parking lots, claiming that his/her AV was lost, when he/she already picked it up before. Additionally, certain involved parties, such as clients, parking lots, or thieves, might possess distinct motives to conceal their misbehavior. First, the adversary, a legitimate client, attempts to send an untraceable message to pickup the AV. As a result, he could use defame the parking lot by saying his AV was lost. A legitimate user

could potentially remain anonymous in order to avoid being compensated if a traffic accident happens, during which his AV was implicated. Second, the parking lot is more inclined to remain inconspicuous throughout any accident inquiry to minimize complications. Finally, an attacker who steals an AV may prohibit the authorities and the client from locating the vehicle.

That is why the researchers proposed authentication schemes to address these concerns and facilitate the implementation of automated valet parking protocols. Reference [52] proposes a parking protocol that is supposedly automated and secure to protect against vehicle hacking or theft. They proposed two-factor authentication using a one-time password (OTP) and a smartphone was introduced to protect remote control of AVs and defend against malicious access. Hence, an adversary using a smartphone alone or one-time password will not be able to control the AV or steal it. Using the BBS+ signature [59] and the Cuckoo filter [60], they were able to ensure anonymous authentication between clients and automated parking systems, as well as user location privacy preservation. The proposed scheme enhances automated parking services by assisting users in securely connecting to their AVs and securing all transcripts without compromising clients' privacy. Additionally, a judge is responsible for tracing anonymous clients to prevent misdeeds during vehicle pickup or relocating AVs to assist authorities in locating missing AVs with the permission of their owners. Moreover, that judge has authority to retrieve the parking lot, in which some AV is parked for its owner if his/her smartphone was stolen or lost. However, the paper needs to develop strong intrusion detection techniques and strengthen the AV's control systems to secure the vehicle against security threats and attacks.

On the other hand, the researchers in [53] decided to tackle the "Double-Reservation Attack" while maintaining the user's privacy. Their proposed system allows the client to reserve only a single parking space at a time and prohibits one user from making more than one booking and hold multiple parking spots simultaneously. Moreover, they aimed to ensure pseudonymity and unlinkability, that is a painless but effective technique to protect privacy of users. Pseudonymity means that the automated parking system will not have knowledge of the user's unique id that creates a certain booking/parking request. That is except for the registration phase, during which a client have to divulge his/her real id to the automated parking system to validate himself/herself as a legitimate user. Unlinkability means that the automated parking system would not be able to match up a client's two parking bookings, even when knowing the credentials of these tow sessions. Besides, they aimed to ensure geo-indistinguishability by using a mechanism to obfuscate the tracing data of the users to protect him/her from attacks that analyze location statistics in the automated parking system. And finally, they sought to study the system's efficiency, as well as communication cost and computational performance.

The problem of parking lot payment is also being examined. The users must pay to park their cars using the smart payment system [54]. In the beginning, the currency is collected using cash counters, but they are difficult to maintain. After that, a variety of methods are employed to collect the money. Payment is made using the Automated Vehicle Identification (AVI) tag, based on RFID technology. RFID and mobile devices are contactless technologies, whereas smart cards, debit cards, and credit cards are contact methods.

Additionally, there is the problem of fleet management in AVs. Often, a company would have more than one vehicle running around the city for various errands. They all have to park somewhere, not necessarily all in the company's same parking lot. In that case, a plurality of parking spaces is needed to be assigned, keeping in mind the current location of the vehicles and their tasks for the next day. Therefore, a fleet parking system is being investigated by researchers, such as in [61], where they developed an algorithm to produce a total cost function and cost value to the decision-maker to help choose the best fleet parking scenarios.

On the other hand, the security of ultrasonic sensors heavily involved in the parking process was investigated in [55]. These sensors detect hurdles by releasing ultrasounds and examining their reflections. Some attackers may exploit their operation to introduce spoofing or jamming attacks, thereby causing the AV to stop when it should be moving or the other way around, which may lead to collisions. Therefore, they proposed two protection methods. The first one is a single-sensor-based, which provides physical shift authenticates (PSA). The second method uses multiple sensor consistency check (MSCC), which verifies various signals on the system level. They tested their work on the autopilot system of a Tesla Model S car.

The following sections will investigate further security attacks on the system and physical levels. But in short, the previous ideas are just a sample of how one application may have numerous ideas being developed, and hence, multiple privacy and security issues will arise accordingly, which will need to be handled in more innovative ways. Systematic design strategies on different levels are needed to enhance the overall systems' security and reliability against future threats. Striking a balance between location privacy and the optimal utilization of parking lots is a crucial problem. In Table 4 we show a brief digest of the aforementioned ideas and our corresponding comments.

5) INTERNET OF VEHICLES

Another application worth investigating is using the vehicle itself equipped with all sorts of sensors as a sensor platform, which collects information from the environments and neighboring vehicles and feeds this information to some system to assist in various smart city data repositories such as traffic management and pollution control. This so-called Vehicle

TABLE 4. Security & privacy attacks on parking applications.

Ref. No.	Threat	Proposed Method	Critique
[52]	Vehicle hacking or theft	Two-factor authentication, OTP and a smartphone	Lacks strong intrusion prevention techniques and needs to strengthen the AV's control systems.
[53]	Double Reservation Attack	One parking spot Per user, pseudonymity and unlinkability and geo-indistinguishabili by data obfuscation	Doesn't account for theft, sabotage or slandering.
[54]	Fraudulent payment	Smart payment system using AVI and RFID	Contactless payments can be hackable without any physical trace.
[55]	Spoofing and jamming the ultrasonic sensors	PSA and MSCC	Susceptible to wide-band jamming attacks and attackers collusion.

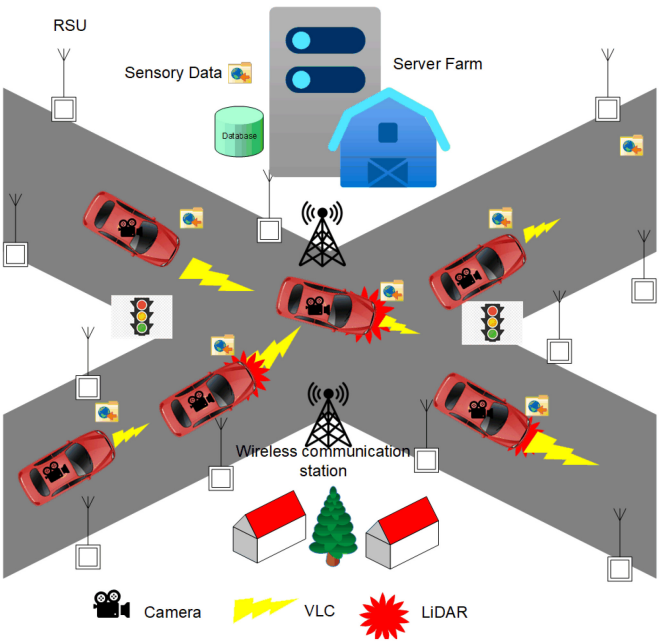

FIGURE 6. Architecture of IoV system.

Grid fundamentally evolved into an Internet of Things (IoT), which is conveniently called the Internet of Vehicles (IoV).

As shown in Figure in 6, IoV incorporates many so-called "things", for example:

- *Vehicle's beacons:* Alarming devices which monitor the AV state; such as location, internal parameters, potential hazards, etc.
- *Driver's messages:* Such as social media posts and other crowdsourced info.
- *Internal cockpit sensors:* Such as the driver's state of tone of voice, alertness, seat position, health, and other propriety sensors such as Ford heart Monitor, etc.
- *Internal automotive sensors and actuators:* Such as accelerator, steering wheel, brakes, etc.
- *External sensors:* Such as lidars, cameras and GPS,.. etc.

The differences between IoV and other IoTs are the following characteristics: I. Sensors are mobile, which may cause a wireless communication bottleneck while guaranteeing motion privacy. II. Some information will be used in safety-critical applications, which requires small latency. Moreover, IoV doesn't transfer data to the Internet using the Internet connection only. Additionally, It utilizes vehicle-to-vehicle communications to complement onboard sensor data and bring forth safe and orderly navigation. However, such continued information collection may create privacy and security violations, which need to be addressed. More specifically, researchers should focus on guaranteeing location privacy and offer privacy-keeping methods to anonymously upload sensor data from AVs.

In [17], the authors studied the IoV system. An attacker may use the size of the database to determine whether a certain targeted user is included. As a result, the size of the database or the total number of users shouldn't be publicized. To ensure the confidentiality of the shares, data owners would establish an individual Transport Layer Security (TLS) connection to each aggregator. The TLS connection is designed to be long-lived in order to compensate for connection initialization costs. While aggregation delegates may attempt to conspire, it was considered in this scheme that at the minimum one truthful aggregate delegate wouldn't conspire. Additionally, data contributors can attempt to conspire with aggregators; thus, they presume that at minimum two trustful data contributors do not conspire with aggregators. The more trustworthy data contributors there are, the greater privacy protections for data contributors. Aggregation servers are anticipated to be online and continually available, and they did not account for DoS attacks, in which data owners' responses are unable to be transmitted. Additionally, the paper assumes aggregators do not corrupt data.

In [62] the researchers provided an authentication technique to secure AV users' privacy. Their proposed system addressed previous work [66] shortcomings in terms of location spoofing, offline identity guessing attacks, and reply attacks. Their work presented a defense against impersonation and DoS attacks, using a lightweight encryption and hashing scheme.

In [63], the authors design a secure authenticated key management protocol for IoV (AKMIoV) based on fog computing. They use road units equipped with fog computing platforms and cloud servers to provide secure communications for the vehicles using secure session keys among all these parties. They performed a security analysis of their system using the "Real-Or-Random (ROR)" model, as well as the Automated Validation of Internet Security Protocols and Applications (AVISPA) model. They showed that this

TABLE 5. Security & privacy attacks on IoV applications.

Ref. No.	Threat	Proposed Method	Critique
[17]	Compromising user privacy	TLS	Doesn't count for DoS attacks and data corruption.
[62]	Location spoofing, identity guessing attacks and reply attacks	lightweight encryption and hashing	They didn't account for intrusion. Storage cost is quite considerable. They didn't consider communication overhead.
[63]	Attacks on user authentication	AKMIoV and fog computing	Entails more setup cost to equip RSUs with powerful computing devices and assumes there would be continuous communication channles between all parties. Also, scalability and management becomes an issue.
[64]	Compromising location privacy	Fog computing supported IoV, P3	Entails more setup cost to equip RSUs with powerful computing devices. They didn't consider intrusion attacks on the RSUs. Scalabity is also an issue with sparse number of AVs.
[65]	Voting collusion	Blockchain- enabled IoV	Susceptible to fraudulent submissions which may compromise voting process. Also, the heave computation overhead.

new method supersedes comparable techniques in terms of enhanced computation cost, network throughput, packet loss rate and end-to-end delay.

Fog computing was also used in the work of [64]. The paper presents a model called F-IoV, which stands for fog computing supported IoV. This model aims to effectively manage networked resources in the IoV, utilizing the roadside infrastructure. In addition, they proposed a hierarchical privacy-preserved pseudonym (P3) scheme, which provides a context-aware pseudonym changing game. Also, their analysis showed effectively enhanced location privacy with reduced pseudonym management and communication overhead.

The use of blockchain technology was also investigated in the field of IoV. In [65], the authors introduced a blockchain-enabled IoV (BIoV) to ensure the security and traceability of the shared data. Their focus was to defend against voting collusion between candidate data miners by securing the selection process by a reputation-based voting scheme that examines historical interactions and recommendations from other vehicles. In addition, the paper introduced a block verification scheme to defend against internal collusion among active miners. This verification is audited by standby miners, who will be incentivized to participate using a contract theory model.

In [67], the authors took a new direction and investigated the problem of digital forensics investigations in IoV. In AV, this problem becomes more difficult due to AVs' distributed and dynamic nature in an IoV; hence collecting and analyzing evidence may be more difficult. The authors presented the TrustIoV framework to collect and store trustworthy evidence from the decentralized infrastructure of IoV while maintaining the integrity of data and its provenance with minimal overhead.

In summary, unlike some of the previous applications, in the context of AVs, the field of IoV is relatively new. Hence it is ripe with an open area for research and development [68]. Security requirements should be balanced with energy efficiency, communication overhead, and safety requirements [69]. In addition, ongoing research should focus on migrating from traditional operating systems models to new middleware platforms, which could enable proper and secure handling, processing, and analytics of data generated in IoV, which may grow to the level of so-called big data [70]. A synopsis of the work discussed here and our related critique is shown in Table 5.

6) AUTONOMOUS VEHICLES CLOUD COMPUTING

The computing power of AVs is quickly increasing. AVs are outfitted with different processing, memory, storage facilities, and computer vision technologies. Researchers took the computing potential found in AVs to the next level. They aim to utilize these smart cars' occasionally inactive computing capabilities to provide computing services as a utility. This model is called autonomous vehicles cloud computing (AVCC) [75]. Cloud computing is a relatively new technology that is currently game-changing in the industry. Users don't need to own powerful computing capabilities at their hands. Instead, they can rent as much power as they need in a pay-as-you-go model. The advancement in communication technologies such as LTE and 5G allows a gradually ubiquitous spreading of this new paradigm. Cloud computing is being offered in different delivery models suiting different user needs. There is Software as a service, Platform as a service, and Infrastructure as a service. These models have something in common; some computation task is done remotely in a physically out-of-reach platform that the user cannot control or govern. Remote code execution is a trending requirement in numerous usage scenarios, such as a case when a user is using a smartphone or a small computer. In other situations, some companies opted to use cloud computing platforms to allow their employees a more flexible working style. In times of hardship like nowadays, the pandemic forced many people to work from their homes, and they needed to access the company's computing resources seamlessly with the same functionalities. On the other hand, these usage scenarios suffer from common security threats and privacy concerns. More importantly, remote code execution on shared platforms that are physically inaccessible is inherently risky in terms of trustworthiness. That is to be confidential, integral, and available at time of need.

TABLE 6. Security & privacy attacks on AVCC applications.

Ref. No.	Threat	Proposed Method	Critique
[71]	Compromising user privacy	CP-ABE	Entails heavy computations and communication overhead, especially during the start up and key distribution phase.
[72]	Compromising user privacy and authentication	Hierarchical ABE	System is exposed to too many parties, and there are many privacy concerns. Additionally, having to deal with the complicated system of attribute distributions.
[73]	Attacks on user authentication	Biometric and ECC-assisted authentication	ECC involves heavy computations and therefore consumes a lot of power.
[74]	Attacks on user authentication	Single-server 3-factor AKA protocol and the non-interactive identity-based key establishment protocol	The centralized server becomes a single point of failure, also there is more communication overhead.

These requirements become more challenging in the field of AVCC. Although AVCC is essentially a cloud computing platform, using cars instead of stationary computers residing in some company's buildings introduced more challenging problems. The first obvious problem is that these cars are moving, which means that the communication interfaces will continually change the cloud formation. Although the organizational problems are addressed from an architectural perspective, they open the system to unknown threats every time a car enters or leaves the cloud [76]. Secondly, AVs are powered by embedded systems, which means they have power limitations and limited processing capabilities, storage, and memory.

Although AVCC is a fairly new paradigm, it's based on the VCC and VANET technologies. Therefore, it inherited their problems and security concerns. Such as DoS, jamming, hijacking authentication, racketeering, copyright infringements, stealing data, sabotage, and information leakage via side-channels and reverse engineering [86]. Fortunately, some of the approaches to mitigate these issue seem relevant as well her and can be applicable.

In [71] the authors propose an algorithm to ensure VCC security and privacy. They use Pseudo-ID instead of vehicles' real ID to provide conductors' privacy, Identifier-Based Signature mechanism is used to guarantee vehicles' authentication, and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) algorithm is used for key distribution. They claim that their liGhtweight secURe AutheNticaTion and keY distribution scheme for vehicular cloud computing (GUARANTY) ensures a secure keys distribution to minimize the encryption and decryption computation cost. In their scheme, vehicles use a symmetrical cryptography in their communication. But in our opinion their system does entail some heavy computations and communication overheads, specially during the start up and key distribution phase.

In [72] the authors propose SmartVeh, as a secure and efficient message access control and authentication scheme in VCC. It uses a hierarchical, attribute-based encryption technique to achieve fine-grained and flexible message sharing, which ensures that vehicles whose persistent or dynamic attributes satisfy the access policies can access the broadcast message with equipped on-board units (OBUs). Additionally, Message authentication is enforced by integrating an attribute-based signature, which achieves message authentication and maintains the anonymity of the vehicles. In order to reduce the computations of the OBUs in the vehicles, they outsource the heavy computations of encryption, decryption and signing to a cloud server and road-side units. Nevertheless, we fear that their system is exposed to too many parties, and there are many privacy concerns. Additionally, having to deal with the complicated system of attribute distributions comes with computational overhead and communication cost. Relying on a cloud server for doing these computations is not always practical, and may present a new attack surface.

The authors in [73] propose a biometric and elliptic curve cryptography (ECC)-assisted authentication framework for VCC. They claim that their presented framework obtains most of security features and attributes for secure communication in the presence of active and passive attackers. Further, They provide formal security model and its proof, which is based on random oracle model. Also, they compare the performance of their protocol with similar frameworks in the same environment in terms of communication and computation overheads.

In [74] the researchers present an integrated Authentication and Key Agreement (AKA) framework for vehicular clouds. They integrated the single-server 3-factor AKA protocol and the non-interactive identity-based key establishment protocol, and evaluated its performance based on a simulated experimental platform. The authors in [87] discussed the construction of the authenticated session key agreement protocol for vehicular cloud. They claimed that their proposed framework also maintains the anonymity of participating vehicles. In Table 6 we briefly discuss and comment on the ideas mentioned in this subsection.

III. OPERATING SYSTEM LEVEL

Due to the continual progress and enhancement in deep learning (DL) technology, AVs have achieved remarkable advances in recent years. On several standard autonomous driving systems, X86-based software performs sophisticated functions and contributes significantly to driving safety. However, software vulnerabilities in autonomous driving might compromise vehicle components and systems, which impair the AVs' performance.

TABLE 7. Security & privacy attacks on the operating system level.

Ref. No.	Threat	Proposed Method	Critique
[77]	Malware	OTA updates	Susceptible to tampering and cloning.
[78]	Attacks on remote OTA updates	Encryption keys [79], [80], [81], [82] or blockchain [83]	Each technique has it's own performance cost in terms of computation overhead, communication cost and power consumption.
[84]	Malware	Cloud-based protection	Requires a continuous communication link between the vehicle and the cloud (a bottleneck for Network attacks).
[85]	Malware	Machine learning with fusion features	Requires huge computations, and doesn't support dynamic analysis of threats.

In [77], the authors studied malware attacks on AV systems. They investigated an attack that exploits the onboard device (OBD) and thereafter targets electronic control units (ECUs) and its connected CAN bus. They also exploit mobile apps to access the DSRC. The target of these attacks can be any of the AV system's various software components, such as OBD ports, software Over-The-Air (OTA) updates, ECU firmware, . . . , etc. The paper also discussed different approaches to defend against these attacks, such as offering OTA updates, but these techniques may also open the system to a new attack surface; therefore, these updates need a great deal of work to protect it against tampering and/or cloning.

In [78], the authors focused on remote OTA updates and their security issues. They also studied various scenarios and regulations of road safety in different nations. Some of these security techniques relied on cryptographic authentication and encryption keys such as [79], [80], [81], [82] others use blockchain such as [83].

Other techniques to defend against malware attacks incorporate a much more capable cloud-based protection. In [84], the authors present a cloud-assisted vehicle malware defense framework. The paper proposed a lightweight malware defense mechanism that resides on the vehicle. At the same time, the heavy and much-advanced processing is done over a cloud with an up-to-date malware information database. However, adding a continuous communication link between the vehicle and the cloud might be a bottleneck that could open the system to a whole new network-level breed of attacks, which we will delve into with more details in the following section.

Additionally, numerous researchers have developed static and dynamic analysis techniques to uncover malware on embedded system components based on the X86 architecture. Static methods examine an input program from a semantics and syntax perspective without executing the software. These techniques offer the advantages of rapid detection and a small percentage of false positives. Nonetheless, a typical limitation of static analysis techniques is their impotence to detect malware that employ sophisticated mechanisms like cryptography, compression, packing and obfuscation.

Dynamic analysis-based techniques can resolve the issue by executing the subject program and observing process creation, memory access, file writing/reading, network utilization and system calls during the runtime of the program. Nevertheless, the dynamic analysis method is resource-intensive, and parallel processing is inefficient in actual applications.

In [85], the authors presented a hybrid malware detection technique that combines machine learning with fusion features from three distinct levels of static analysis. The purpose is augment static analysis's low accuracy and to address dynamic analysis's high resource cost. They developed a model for feature extraction depending on the level of operation. Additionally, to improve the accuracy of static analysis, the authors built a set of tools to unpack codes with various packing methods. Also, they present a novel model using the control flow graph and information entropy for extracting OpCode features. Their technique was established on Extreme Gradient Boosting (XGBoost). Which in comparison with other popular classification algorithms, achieves a greater accuracy in recognition.

On the other hand, despite their enormous potential, AVs supported by DL technology continue to confront several system-level security concerns. The authors of [27] focused on traffic sign recognition system and they leveraged particle swarm optimization to undertake attacks that target their deep learning algorithms. The paper first exploits the "poisoning attack with particle swarm optimization" (PAPSO) attack, that targets the deep learning algorithms during the training phase. During which malicius samples are implanted in the input data by the attacker, reducing the traffic sign recognition system's classification accuracy. Additionally, the authors investigate the "evasion attack with particle swarm optimization" (EAPSO), that target the deep learning algorithms' interference process. Attackers introduce certain barely noticeable changes to the selected test sample, resulting in misclassification. Table 7 depicts an abridgment of the literature shown in this subsection as well as our critique to them.

IV. NETWORK LEVEL

Vehicular networks (VNs) are gaining huge attention as a research area due to the importance of aiding traffic management and providing road safety. Nowadays, many communication interfaces are integrated in Vehicles, this demands installing processing hardware, storage elements and larger power sources. In addition, to aid with traffic management system, road side unites are deployed, to communicate with vehicles wirelessly.

These systems can support taking preventative safety actions for the sake of vehicle commuters and drivers, as

TABLE 8. Security attacks on vehicular networks and their countermeasures.

Service	Attacks	Countermeasures
Availability	Malware	Digital Signature of Software, Reliable Hardware
	Spamming	Digital Signature of Software, Reliable Hardware
	Greedy Behavior	Intrusion Detection Systems
	Blackhole and Grayhole	Digital Signature of Software, Reliable Hardware
	Broadcast tampering	Cryptographic Primitives
	Jamming	Frequency Hopping, Direct Sequence Spread Spectrum
	Denial of service	Signature Based Authentication
Confidentiality	Man In the Middle	Digital Certificates
	Traffic Analysis	Encryption Techniques
	Social	Digital Signature
	Eavesdropping	Physical Layer security Protocols
Authenticity	Sybil	Central Validation Authority, location and Position Verification
	Tunneling	Digital Signature of Software, Reliable Hardware
	GPS Spoofing	Signature authentication, trusted positioning systems, bit commitment
	Free-riding	Strong Authentication
	Key and/or Certificate Replication	Certified Keys, Validate Certificates in Real Time
Integrity	Masquerading	Digital Signature of Software, Reliable Hardware
	Reply	Digital Signature
	Illusion	Digital Signature of Software, Plausible Validation Network
	Message Tampering	Zero-Knowledge Schemes
Non-Repudiation	Repudiation	Identity Based Signature, Digital Certificates

well as aid traffic authorities. Several methods have been proposed for discussing the security and privacy issues for VNs and vehicular cloud computing (VCC).

It is essential to fulfill the security requirements in a vehicular network, which we explain in more detail as follows.

- *Availability:* Means that the system can withstand malicious or erroneous circumstances and still ensures it's functionality [88]. That's why this requirement is susceptible to wider attack types in comparison to other security requirements. Reference [89] describes some countermeasures such as encryption techniques and trust mechanisms to defend against some of these attacks.
- *Confidentiality:* Means that only a specified/delegated user can access his/her data that he has legal authority/rights to do so. Others who don't, cannot access said data.
- *Authentication:* Means that only pre-identified and authorized users can access the network and pass messages. Other malevolent parities or intruders are denied from access [90].
- *Data Integrity:* Means that we ensure the correctness of the messages being passed from unintended alterations or modifications while being passes throughout the network. There are some techniques to ensure data integrity such cryptography revocation and public key encryption [89].
- *Nonrepudiation:* Means that in case of a dispute, both communicating parties: the sender and the recepient cannot repudiate their action [91], [92].

A survey of AV communication layers and its security challenges is presented in [93]. The paper shows how conventional vehicular ad hoc network (VANETS) has metamorphosed to a contemporary paradigm coined the Internet of Vehicles (IoV) - aligned with the advancement in Internet of Things (IoT) systems and will soon evolve into the Internet of Autonomous Vehicles (IoAV).

Table 8 shows an illustration of different attacks on these communication aspects of the VN and exemplary countermeasures to tackle some of these attacks [94], [95], [96], [97].

In [98], the authors studied the effects of security vulnerabilities and risks associated with deploying VANET communication and tampering of automated sensing and control of "Cooperative Adaptive Cruise Control (CACC)", which describes a stream of vehicle connected together and cooperating together. The authors showed how an attacker can compromise CACC systems. They used an open-source software "Vehicular Network Open Simulator" (VENTOS), to implement a CACC car-following model. The model was utilizing IEEE 802.11p to simulate one vehicle look-ahead communication in VENTOS. Hence, they were able to provide a quantitative analysis of a variety of what-if cases that describe security onslaughts on the CACC system. The paper also discussed some important security consideration than needs to be contemplated in design to warrant the system's safety by performing a detailed packet-level analysis.

Another major issue that targets traffic systems is Sybil attacks, during which an attacker could impersonate a number of cars that pass on an untruthful incident down the road. Typically a traffic system needs information about any events to alert vehicle operators of unforeseen dangers on the roads to provide safe driving.

The authors in [99] proposed a security model to protect VNs based on Integrated Circuit Metric technology (ICMetrics). This ICMetrics is utilized to provide a robust authentication scheme based on distinctive features extracted from vehicle sensors and its behaviour. In particular, they studied a simulated VANET and examined the resulting trace file, looking for infrared sensors' bias values. Thereby their

system can identify abnormal behavior that could mount to be a malicious attack.

On the other hand, the researchers in [100] studied intrusion attacks and their countermeasures in AVs. They classified VN into two categories: Intra-vehicle networks and Inter-vehicle networks. The first category, networks that operate on the "intra-vehicle" level, connect cars to the outside world, including all external devices, usually through wireless interfaces such as Wi-Fi, GSM, LTE ... etc. ECU fabricated in the car supports these communication interfaces using technologies that support different types of sub-networks. The most used sub-networks are FlexRay, Local Controller Area networks (CAN), Interconnect Networks (LIN) and Media Oriented Systems Transport (MOST) [101]. In the intra-vehicle networks, some of the most common intrusion attacks targeted Web browsers on the cars system, the telematics units, or the broadcast messages [102], [103]. In order to tackle these attacks, the authors suggested the use of cryptographic techniques as in [104], [105], secure hardware implementations for the ECU such as [106], the infrastructure of the AV as in [107], and finally employing mechanisms for anomaly detection as in [108], [109], [110].

On the other hand, Inter-vehicle networks are famously known as VANET, where communication happens between the vehicles (V2V). Here the attacks can be launched from inside or outside of the network, and they could be active or passive attacks. They may cause a denial of service, inject bogus information, steal the identity of some user or part of his information like his speed or position, and last but not least, racketeering and digital piracy. More details about these attacks and their countermeasures can be found in [111], [112], [113].

V. PHYSICAL LEVEL

AVs are equipped with various sensors that enable them to monitor the surrounding environments and navigate safely. One of the most direct and upfront physical level security threats are attacks against these sensors. Attackers may produce incorrect information messages or ultimately hinder sensor operation to disrupt autonomous driving without accessing the AV's driving system. There are many attack surface vectors according to the sensor type [117]. For instance, AVs are commonly fitted out with numerous cameras with a variety of lenses for object detection and tracking. Here, attackers plant fake traffic signs or lights, or even some kind of objects, to spoof AVs and drive them into wrong decisions [118]. The attacker may also use a very bright laser beam to blind the camera, thus preventing it from taking any images [117], [118]. In addition to that, AVs use global navigation satellite systems and inertial navigation system sensors to learn their location in real-time. The attacker may use noise signals to interfere with the sensor's receivers to jam it. Furthermore, they may spoof location messages and tamper with them [117], [118].

On a related issue, the continued expansion of electronic device cloning poses a severe threat to any essential infrastructure that relies on the Internet, such as AVs, because cloned devices might send secret data and create security issues. Also, cloned devices could be untrustworthy since they might be built using substandard materials and may have numerous flaws due to insufficient testing. Thus, it is critical to secure these electronic devices against cloning. Preventing a device from being cloned is as simple as avoiding copying the firmware. In the absence of the correct firmware, the machine would not operate in the same manner as the original. As conventional cloning protection solutions, such as: integrity checking and firmware encryption, are prohibitively expensive in development costs. Also, during execution, they consume a lot of resources consumption on oftenly resource-constrained devices. That is why, more than ever, we urgently need low-cost solutions.

The authors of [114] examined two types of security attacks. In the first level (Level-I), a microcontroller serves as an interface device programmed using a serial wire debug (SWD) interface's driver and the UART module. The interface communicates with the subject device through the SWD and controls its reset and power connections. While the subject device completes cyclic redundancy check, the interface device reads the SRAM, controls the subject's d power, and resets if needed. A script (implemented in Python) runs on the computer communicates with the interface via UART, and snapshots from the SRAM of the interface device can be transmitted to the laptop for firmware extraction. While this Level-I protection can be disabled, the flash memory is erased, thus hindering the extraction of the firmware by an attacker. The second level of protection (Level-II) considers attacks that target the microcontroller invasively. Following decapsulation, memory protection bits are reprogrammed by using some specific ultraviolet light [91]. After reprogramming, the Level-I attack mentioned above can be launched and the firmware can be extracted from the victim. Level-II locks the debug interface completely and irreversibly, allowing just processor's cores access to the flash memory.

Additionally, the authors introduced a new firmware obfuscation technique that has a low cost for detecting cloned systems successfully. Obfuscation of the firmware is accomplished by reordering a number of chosen instructions. The native instruction flow is disrupted by an efficient technique to obfuscate the firmware's original execution sequence. Their approach begins with a single instruction and searches for a collection of swappable instructions to ensure that no faults are encountered. Their approach will not stop an attacker from stealing the firmware, in lieu making it operational ultimately as well as providing reasonable cloning protection. Additionally, they built a mechanism for tamper resistance. Specifically, they explain how it is impractical to rebuild the original firmware by an attacker, taken into account the available computing resources, making their mechanism a good candidate in securing "cyber-physical systems (CPS)" and IoT applications such as AVs.

TABLE 9. Security & privacy attacks on the physical layer.

Ref. No.	Threat	Proposed Method	Critique
[114]	Level-I and Level-II attacks on the microcontroller to extract firmware	Firmware obfuscation	Will not prevent stealing hardware, it's hard but not impossible for an attacker with sufficient dynamic analysis resources to reverse engineer the code.
[115]	System Failures and compromising AV cyber-security lifecycle.	STPA method and the Six-Step Model	System is too complicated and Needs more refinement to be applicable. Also, need to consider scalabity and collaborative scenarios.
[106]	Attacks on the ECU	Holistic HSM	Although the model might be tailored to guarantee in-vehicle specific requirements, this might hinder its scalability and wide, general purpose industrial applicability.
[116]	Intrusion attacks	Various IDS according to vehicle type and access methods	Each technique has its pros and cons. As such, some might need physical audit features, others may require more generalized hardware design considerations.

Another interesting piece of work is [115], where the authors presented a six-step model that utilizes System-Theoretic Process Analysis to ensure both the safety of the vehicle and its passengers as well as the security requirements. They claimed that their approach is compliant SAE J3016, SAE J3061, and ISO 26262 all of which are international standards.

In [106] the authors focused on securing vehcile ECUs and their communications. They proposed a holistic hardware security model (HSM) and offered details on a prototype implementation. Their model aim is to act a as trusted security anchor which can generate, store, and process information protected from malicious software. It should also resist hardware tampering attacks and support cryptographic hardware operations all of which presented in a highly optimized special hardware prototype.

The authors in [116] presented a survey and classification of intrusion attacks on vehicles and their detection methods. They studied intrusion detection systems (IDS) in different types of cyber-physical systems such as AVs, UAV ans autonomous ships. They also investigated on-board physical attacks and their countermeasures as well as remote and network-based intrusion attacks and also their mitigation strategies along with their advantages and disadvantages. Their eventual goal was to shed some light on the shortcoming of some of the current literature and show directions for future research.

In Table 9 we summarize the literature presented in this section and mention some brief comments about them.

VI. RELATED WORK

There has been a great deal of literature surveying many security aspects of AVs. Some earlier work only focused on the network part, such as [90], [95] and [94]. Others focused on one of the security issues related to one of the applications discussed in Section II. For example, the authors in [17] investigated numerous of applications that utilize V2I and V2V platforms and connections. They also describe location privacy issues related to users' mobility. They showed the necessity of building openly and publicly accessible, "smart city" data repositories available for all researchers as well as offer privacy-keeping schemes to enable vehicles to upload urban sensor data anonymously. In addition, the authors in [10] studied the viability of guaranteeing preserving privacy along with safety and integrity in the new hyper-connected vehicular platforms. To prove that point, they studied a scenario where vehicles upload their map updates while keeping their privacy as well as the integrity of their messages.

That said, the contribution of this paper is to survey AV privacy issues and security challenges from a multi-layer perspective. We tackled these problems within each layer and showed some state-of-the-art work to solve them. We hope that this big picture view would help develop solutions that would address several issues simultaneously and support the spread of AV technologies.

VII. CONCLUSION

AI is gradually changing the technological services we use in our everyday life. Among which is smart transportation, coined AVs. These new machines are smart, and they know a lot of information about their users. They utilize this information to provide new attractive offerings and protect passengers from imminent dangers among other things. But the problem is that the collection of all that data presented new security and privacy attack surfaces that need to be appropriately handled. This paper surveyed these security and privacy issues in a layer-based model. We vision the AVs system as consisting of four layers, and we investigated some of the attacks on each layer and some of the most promising corresponding countermeasures. Our goal is to help researchers from a different backgrounds identify where they can contribute in this vivid field.

In summary, we discussed open research directions, showed some gaps in existing literature and paved the way for future work. Hence, we plan to focus on some areas of this interesting field, perhaps one of the AV promising applications and hopefully contribute to its privacy and security. We also plan to evaluate our ideas in more realistic environments and against a wider range of attack scenarios.

ACKNOWLEDGMENT

This research work was financially supported in part by NSF CNS 1852126. In addition, parts of this paper, specifically Sections I, II, IV, and V, were made possible by NPRP grants NPRP13S-0205-200270 from the Qatar National Research

Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

REFERENCES

[1] "Road Traffic Injuries and Deaths." Center of Disease Control (CDC). [Online]. Available: https://www.cdc.gov/injury/features/global-road-safety/index.html (Accessed: Mar. 30, 2022).

[2] D. J. Glancy, "Privacy in autonomous vehicles," *Santa Clara Law Rev.*, vol. 52, no. 4, p. 1171, 2012.

[3] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*, vol. 1. Chichester, U.K.: Wiley, 2009.

[4] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, 2014, pp. 241–246.

[5] M. Zangui, Y. Yin, and S. Lawphongpanich, "Sensor location problems in path-differentiated congestion pricing," *Transp. Res. C, Emerg. Technol.*, vol. 55, pp. 217–230, Jun. 2015.

[6] S. B. Raut and L. Malik, "Survey on vehicle collision prediction in VANET," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res.*, 2014, pp. 1–5.

[7] S. Berghaus and A. Back, "Requirements elicitation and utilization scenarios for in-car use of wearable devices," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, 2015, pp. 1028–1037.

[8] S. Hess, A. Meschtscherjakov, T. Ronneberger, and M. Trapp, "Integrating mobile devices into the car ecosystem: Tablets and smartphones as vital part of the car," in *Proc. 3rd Int. Conf. Autom. User Interfaces Interactive Veh. Appl.*, 2011, pp. 210–211.

[9] V. L. Thing and J. Wu, "Autonomous vehicle security: A taxonomy of attacks and defences," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, 2016, pp. 164–170.

[10] S. Karnouskos and F. Kerschbaum, "Privacy and integrity considerations in hyperconnected autonomous vehicles," *Proc. IEEE*, vol. 106, no. 1, pp. 160–170, Jan. 2018.

[11] B. A. Forouzan, *TCP/IP Protocol Suite*. New York, NY, USA: McGraw-Hill, 2002.

[12] H. Zimmermann, "OSI reference model-the ISO model of architecture for open systems interconnection," *IEEE Trans. Commun.*, vol. 28, no. 4, pp. 425–432, Apr. 1980.

[13] S. Chuprov, I. Viksnin, I. Kim, L. Reznikand, and I. Khokhlov, "Reputation and trust models with data quality metrics for improving autonomous vehicles traffic security and safety," in *Proc. IEEE Syst. Security Symp. (SSS)*, 2020, pp. 1–8.

[14] K. Rabieh, M. M. Mahmoud, and M. Younis, "Privacy-preserving route reporting scheme for traffic management in vanets," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 7286–7291.

[15] R. Hussain and H. Oh, "On secure and privacy-aware Sybil attack detection in vehicular communications," *Wireless Personal Commun.*, vol. 77, no. 4, pp. 2649–2673, 2014.

[16] R. Reshma, T. Ramesh, and P. Sathishkumar, "Security situational aware intelligent road traffic monitoring using UAVs," in *Proc. Int. Conf. VLSI Syst. Archit. Technol. Appl. (VLSI-SATA)*, 2016, pp. 1–6.

[17] J. Joy and M. Gerla, "Internet of Vehicles and autonomous connected car-privacy and security issues," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2017, pp. 1–9.

[18] L. Adacher, A. Gemma, and G. Oliva, "Decentralized spatial decomposition for traffic signal synchronization," *Transport. Res. Procedia*, vol. 3, pp. 992–1001, Dec. 2014.

[19] C. Wuthishuwong and A. Traechtler, "Coordination of multiple autonomous intersections by using local neighborhood information," in *Proc. Int. Conf. Connected Veh. Expo (ICCVE)*, 2013, pp. 48–53.

[20] P. Gora, "Simulation-based traffic management system for connected and autonomous vehicles," in *Road Vehicle Automation*, vol. 4. Cham, Switzerland: Springer, 2018, pp. 257–266.

[21] P. Wagner, "Traffic control and traffic management in a transportation system with autonomous vehicles," in *Autonomous Driving*. Cham, Switzerland: Springer, 2016, pp. 301–316.

[22] I. Rubin, A. Baiocchi, Y. Sunyoto, and I. Turcanu, "Traffic management and networking for autonomous vehicular highway systems," *Ad Hoc Netw.*, vol. 83, pp. 125–148, Feb. 2019.

[23] S. A. Fayazi and A. Vahidi, "Vehicle-in-the-loop (VIL) verification of a smart city intersection control scheme for autonomous vehicles," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, 2017, pp. 1575–1580.

[24] F. Ashtiani, S. A. Fayazi, and A. Vahidi, "Multi-intersection traffic management for autonomous vehicles via distributed mixed integer linear programming," in *Proc. Annu. Amer. Control Conf. (ACC)*, 2018, pp. 6341–6346.

[25] S. El Hamdani and N. Benamar, "Autonomous traffic management: Open issues and new directions," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, 2018, pp. 1–5.

[26] S. Ucar, S. C. Ergen, and O. Ozkasap, "IEEE 802.11p and visible light hybrid communication based secure autonomous platoon," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8667–8681, Sep. 2018.

[27] W. Jiang, H. Li, S. Liu, X. Luo, and R. Lu, "Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4439–4449, Apr. 2020.

[28] "A collaborative approach for improving the security of vehicular scenarios: The case of platooning," *Comput. Commun.*, vol. 122, pp. 59–75, Jun. 2018.

[29] F. Gonçalves *et al.*, "Secure management of autonomous vehicle platooning," in *Proc. 14th ACM Int. Symp. QoS Security Wireless Mobile Netw.*, 2018, pp. 15–22.

[30] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful degradation of cooperative adaptive cruise control," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 1, pp. 488–497, Feb. 2015.

[31] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proc. 10th ACM Symp. Inf. Comput. Commun. Security*, 2015, pp. 167–178.

[32] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy? A study of misbehavior in vehicular platoons," in *Proc. 8th ACM Conf. Security Privacy Wireless Mobile Netw.*, 2015, pp. 1–11.

[33] R. M. Gerdes, C. Winstead, and K. Heaslip, "CPS: An efficiency-motivated attack against autonomous vehicular transportation," in *Proc. 29th Annu. Comput. Security Appl. Conf.*, 2013, pp. 99–108.

[34] D. D. Dunn, *Attacker-Induced Traffic Flow Instability in a Stream of Automated Vehicles*. Logan, UT, USA: Utah State Univ., 2015.

[35] D. D. Dunn, S. A. Mitchell, I. Sajjad, R. M. Gerdes, R. Sharma, and M. Li, "Regular: Attacker-induced traffic flow instability in a stream of semi-automated vehicles," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, 2017, pp. 499–510.

[36] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. L. Cigno, "Plexe: A platooning extension for Veins," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, 2014, pp. 53–60.

[37] M. Nabil, A. Sherif, M. Mahmoud, A. Alsharif, and M. Abdallah, "Efficient and privacy-preserving ridesharing organization for transferable and non-transferable services," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 3, pp. 1291–1306, May/Jun. 2021.

[38] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.

[39] L. Zhu, K. Gai, and M. Li, "Blockchain-enabled carpooling services," in *Blockchain Technology in Internet of Things*. Cham, Switzerland: Springer, 2019, pp. 75–91.

[40] M. Baza, N. Lasla, M. Mahmoud, G. Srivastava, and M. M. E. A. Abdallah, "B-ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1214–1229, Apr.–Jun. 2021.

[41] N. D. Chan and S. A. Shaheen, "Ridesharing in North America: Past, present, and future," *Transp. Rev.*, vol. 32, no. 1, pp. 93–112, 2012.

[42] M. Furuhata, M. Dessouky, F. Ordóñez, M.-E. Brunet, X. Wang, and S. Koenig, "Ridesharing: The state-of-the-art and future directions," *Transp. Res. B, Methodol.*, vol. 57, pp. 28–46, Nov. 2013.

[43] H. Xu, F. Ordóñez, and M. Dessouky, "A traffic assignment model for a ridesharing transportation market," *J. Adv. Transp.*, vol. 49, no. 7, pp. 793–816, 2015.

[44] E. Deakin, K. T. Frick, and K. M. Shively, "Markets for dynamic ridesharing? Case of Berkeley, California," *Transp. Res. Rec.*, vol. 2187, no. 1, pp. 131–137, 2010.

[45] "High Occupancy Vehicle Lanes in Canada." Transport Canada. 2010. [Online]. Available: https://tc.canada.ca/en/corporate-services/acts-regulations/canada-transportation-act-review-report (Accessed: Mar. 30, 2022).

[46] C. F. Daganzo and M. J. Cassidy, "Effects of high occupancy vehicle lanes on freeway congestion," *Transp. Res. B, Methodol.*, vol. 42, no. 10, pp. 861–872, 2008.

[47] E. Lutostanski. "Carema Offers Discounted Rates on Toll 183A." 2014. [Online]. Available: https://communityimpact.com/austin/transportation/2014/02/17/carma-offers-discounted-rates-on-toll-183a-2/ (Accessed: Mar. 30, 2022).

[48] A. Sherif, A. Alsharif, J. Moran, and M. Mahmoud, "Privacy-preserving ride sharing organization scheme for autonomous vehicles in large cities," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, 2017, pp. 1–5.

[49] A. Sherif, A. Alsharif, M. Mahmoud, and J. Moran, "Privacy-preserving autonomous cab service management scheme," in *Proc. 3rd Africa Middle East Conf. Softw. Eng.*, 2017, pp. 19–24.

[50] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 270–282.

[51] L. P. Cox, "Truth in crowdsourcing," *IEEE Security Privacy*, vol. 9, no. 5, pp. 74–76, Sep./Oct. 2011.

[52] J. Ni, X. Lin, and X. Shen, "Toward privacy-preserving valet parking in autonomous driving era," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2893–2905, Mar. 2019.

[53] C. Huang, R. Lu, X. Lin, and X. Shen, "Secure automated valet parking: A privacy-preserving reservation scheme for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11169–11180, Nov. 2018.

[54] J. Chinrungrueng, U. Sununtachaikul, and S. Triamlumlerd, "A vehicular monitoring system with power-efficient wireless sensor networks," in *Proc. 6th Int. Conf. ITS Telecommun.*, 2006, pp. 951–954.

[55] 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.

[56] N. Cheaz, A. Diaz, M. E. Head, and J. H. Kerr, "Delayed parking optimization of autonomous vehicles," U.S. Patent 10 625 733, Apr. 21, 2020.

[57] S. J. Lauffer, J. P. Joyce, D. A. Gabor, S. Abbas, and R. Steven, "Electric parking brake for autonomous vehicles," U.S. Patent 10 549 731, Feb. 4, 2020.

[58] B. Rech *et al.*, "Method for a data processing system for maintaining an operating state of a first autonomous vehicle and method for a data processing system for managing a plurality of autonomous vehicles," U.S. Patent 10 607 422, Mar. 31, 2020.

[59] M. H. Au, W. Susilo, and Y. Mu, "Constant-size dynamic k-TAA," in *Proc. Int. Conf. Security Cryptogr. Netw.*, 2006, pp. 111–125.

[60] B. Fan, D. G. Andersen, M. Kaminsky, and M. D. Mitzenmacher, "Cuckoo filter: Practically better than bloom," in *Proc. 10th ACM Int. Conf. Emerg. Netw. Exp. Technol.*, 2014, pp. 75–88.

[61] P. Colijn, L. A. Feenstra, J. S. Herbach, and K. Patterson, "Fleet management for autonomous vehicles," U.S. Patent A 16 719 302, Jun. 25, 2020.

[62] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of Vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[63] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. Rodrigues, and Y. H. Park, "AKM-IoV: Authenticated key management protocol in fog computing-based Internet of Vehicles deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[64] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 8, pp. 2627–2637, Aug. 2018.

[65] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, Mar. 2019.

[66] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017.

[67] M. M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A trustworthy forensic investigation framework for the Internet of Vehicles (IoV)," in *Proc. ICIOT*, 2017, pp. 25–32.

[68] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of Vehicles: Architecture, protocols, and security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, Oct. 2018.

[69] C. Bala *et al.*, *Beiträge zur Verbraucherforschung Band 9 Der vertrauende Verbraucher: Zwischen Regulation und Information*, vol. 9. Düsseldorf, Germany: Verbraucherzentrale NRW, 2020.

[70] J. Contreras-Castillo, S. Zeadally, and J. A. G. Ibañez, "Solving vehicular ad hoc network challenges with big data solutions," *IET Netw.*, vol. 5, no. 4, pp. 81–84, 2016.

[71] H. Goumidi, S. Harous, Z. Aliouat, and A. M. Gueroui, "Lightweight secure authentication and key distribution scheme for vehicular cloud computing," *Symmetry*, vol. 13, no. 3, p. 484, 2021.

[72] Q. Huang, Y. Yang, and Y. Shi, "SmartVeh: Secure and efficient message access control and authentication for vehicular cloud computing," *Sensors*, vol. 18, no. 2, p. 666, 2018.

[73] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, "SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing," *Int. J. Commun. Syst.*, vol. 34, no. 2, 2021, Art. no. e4103.

[74] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 28–35, May/Jun. 2018.

[75] R. W. L. Coutinho and A. Boukerche, "Guidelines for the design of vehicular cloud infrastructures for connected autonomous vehicles," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 6–11, Aug. 2019.

[76] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, 4th Quart., 2020.

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

[78] S. Halder, A. Ghosal, and M. Conti, "Secure ota software updates in connected vehicles: A survey," 2019, *arXiv:1904.00685*.

[79] S. M. Mahmud, S. Shanker, and I. Hossain, "Secure software upload in an intelligent vehicle via wireless communication links," in *Proc. IEEE Intell. Veh. Symp.*, 2005, pp. 588–593.

[80] K. Mansour, W. Farag, and M. ElHelw, "AiroDiag: A sophisticated tool that diagnoses and updates vehicles software over air," in *Proc. IEEE Int. Electr. Veh. Conf.*, 2012, pp. 1–7.

[81] M. Steger, M. Karner, J. Hillebrand, W. Rom, C. Boano, and K. Römer, "Generic framework enabling secure and efficient automotive wireless SW updates," in *Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2016, pp. 1–8.

[82] K. Mayilsamy, N. Ramachandran, and V. S. Raj, "An integrated approach for data security in vehicle diagnostics over Internet protocol and software update over the air," *Comput. Electr. Eng.*, vol. 71, pp. 578–593, Oct. 2018.

[83] 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.

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

[85] 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.

[86] C. P. García, S. Ul Hassan, N. Tuveri, I. Gridin, A. C. Aldaya, and B. B. Brumley, "Certified side channels," in *Proc. 29th USENIX Security Symposium (USENIX Security)*, 2020, pp. 2021–2038.

[87] S. Rana, D. Mishra, and S. Gupta, "Computationally efficient and secure session key agreement techniques for vehicular cloud computing," in *Advances in Communication and Computational Technology*. Singapore: Springer, 2021, pp. 453–467.

[88] Y. Qian and N. Moayeri, "Design of secure and application-oriented vanets," in *Proc. IEEE Veh. Technol. Conf.*, 2008, pp. 2794–2799.

[89] C. A. Kerrache, C. T. Calafate, J.-C. Cano, N. Lagraa, and P. Manzoni, "Trust management for vehicular networks: An adversary-oriented overview," *IEEE Access*, vol. 4, pp. 9293–9307, 2016.

[90] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.

[91] F. Al-Hawi, C. Y. Yeun, and M. Al-Qutayti, "Security challenges for emerging VANETs," in *Proc. 4th Int. Conf. Inf. Technol.*, 2009, pp. 1–7.
[92] M. Kassim, R. A. Rahman, and R. Mustapha, "Mobile ad hoc network (MANET) routing protocols comparison for wireless sensor network," in *Proc. IEEE Int. Conf. Syst. Eng. Technol.*, 2011, pp. 148–152.
[93] A. Nanda, D. Puthal, J. J. P. C. Rodrigues, and S. A. Kozlov, "Internet of autonomous vehicles communications security: Overview, issues, and directions," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 60–65, Aug. 2019.
[94] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.
[95] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANET security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[96] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 10, no. 6, pp. 379–388, 2016.
[97] M. Muhammad and G. A. Safdar, "Survey on existing authentication issues for cellular-assisted V2X communication," *Veh. Commun.*, vol. 12, pp. 50–65, Apr. 2018.
[98] 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.
[99] K. M. A. Alheeti and K. McDonald-Maier, "An intelligent security system for autonomous cars based on infrared sensors," in *Proc. 23rd Int. Conf. Autom. Comput. (ICAC)*, 2017, pp. 1–5.
[100] S. Boumiza and R. Braham, "Intrusion threats and security solutions for autonomous vehicle networks," in *Proc. IEEE/ACS 14th Int. Conf. Comput. Syst. Appl. (AICCSA)*, 2017, pp. 120–127.
[101] P. Kleberger, N. Nowdehi, and T. Olovsson, "Towards designing secure in-vehicle network architectures using community detection algorithms," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, 2014, pp. 69–76.
[102] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Security Privacy*, 2010, pp. 447–462.
[103] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Security Symp.*, vol. 4. San Francisco, CA, USA, 2011, pp. 447–462.
[104] A. Van Herrewege, D. Singelee, and I. Verbauwhede, "CANAuth—A simple, backward compatible broadcast authentication protocol for CAN bus," in *Proc. ECRYPT Workshop Lightweight Cryptogr.*, 2011, p. 20.
[105] B. Groza, S. Murvay, A. Van Herrewege, and I. Verbauwhede, "LiBrA-CAN: A lightweight broadcast authentication protocol for controller area networks," in *Proc. Int. Conf. Cryptol. Netw. Security*, 2012, pp. 185–200.
[106] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Proc. Int. Conf. Inf. Security Cryptol.*, 2011, pp. 302–318.
[107] P. Kleberger, A. Javaheri, T. Olovsson, and E. Jonsson, "A framework for assessing the security of the connected car infrastructure," in *Proc. 6th Int. Conf. Syst. Netw. Commun.*, 2011, pp. 236–241.
[108] I. Broster and A. Burns, "An analysable bus-guardian for event-triggered communication," in *Proc. 24th IEEE Real-Time Syst. Symp.*, 2003, pp. 410–419.
[109] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A method of preventing unauthorized data transmission in controller area network," in *Proc. IEEE 75th Veh. Technol. Conf. (VTC Spring)*, 2012, pp. 1–5.
[110] N. Kumar and N. Chilamkurti, "Collaborative trust aware intelligent intrusion detection in VANETs," *Comput. Electr. Eng.*, vol. 40, no. 6, pp. 1981–1996, 2014.
[111] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, 2007.
[112] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *Proc. 5th Swiss Transp. Res. Conf. (STRC)*, 2005, pp. 1–14.
[113] G. Samara, W. A. Al-Salihy, and R. Sures, "Security issues and challenges of vehicular ad hoc networks (VANET)," in *Proc. 4th Int. Conf. New Trends Inf. Sci. Service Sci.*, 2010, pp. 393–398.
[114] B. Cyr, J. Mahmod, and U. Guin, "Low-cost and secure firmware obfuscation method for protecting electronic systems from cloning," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3700–3711, Apr. 2019.
[115] G. Sabaliauskaite, L. S. Liew, and J. Cui, "Integrating autonomous vehicle safety and security analysis using STPA method and the six-step model," *Int. J. Adv. Security*, vol. 11, nos. 1–2, pp. 160–169, 2018.
[116] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Netw.*, vol. 84, pp. 124–147, Mar. 2019.
[117] 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.
[118] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," in *Proc. Black Hat Europe*, vol. 11, 2015, pp. 1–13.

MUHAMMAD HATABA (Member, IEEE) received the B.Sc. degree in electronics engineering, majoring in computers and systems from the Faculty of Engineering, Mansoura University, Dakahlia, Egypt, in 2008, and the M.Sc. and Ph.D. degrees in computer science and engineering from the Egypt–Japan University of Science and Technology, Alexandria, Egypt, in 2013 and 2019, respectively.

He is currently with the School of Computing Sciences and Computer Engineering, The University of Southern Mississippi, Hattiesburg, MS, USA. He is also an Assistant Professor with the Computers and Systems Department, National Telecommunication Institute affiliated with the Ministry of Communications and Information Technology, Cairo, Egypt. In 2015, he was a Visiting Research Fellow with the Professor Ueda Laboratory, Department of Computer Science and Engineering, School of Fundamental Science and Engineering, Waseda University, Tokyo, Japan. His research theme was "Code Protection by Obfuscated Dynamic Compilation." His research interests include autonomous vehicles, deep learning, smart grids, and code protection. He has numerous publications in various aspects related to cybersecurity applications. He also has an extensive background in the fields of cloud computing, computer networks, compilers, and software engineering. He is a member of IEEE Computer Society, ACM, USENIX, IEICE, and Egyptian Engineers Syndicate.

AHMED SHERIF (Senior Member, IEEE) received the M.Sc. degree in computer science and engineering from the Egypt–Japan University of Science and Technology in 2014, and the Ph.D. degree in electrical and computer engineering from Tennessee Tech University, Cookeville, TN, USA, in August 2017. He is an Assistant Professor with the School of Computing Sciences and Computer Engineering, University of Southern Mississippi, USA. He is the author of numerous papers published in major IEEE conferences and journals, such as IEEE International Conference on Communications, IEEE Vehicular Technology Conference, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, and IEEE INTERNET OF THINGS JOURNAL. His research interests include cybersecurity; security and privacy-preserving schemes in autonomous vehicles, vehicular ad hoc networks, Internet of Things applications, and smart grid advanced metering infrastructure network. He served as a Reviewer for several journals and conferences, such as IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE INTERNET OF THINGS JOURNAL, and the *Peer-to-Peer Networking*.

MOHAMED MAHMOUD (Senior Member, IEEE) received the Ph.D. degree from the University of Waterloo in April 2011. From May 2011 to May 2012, he worked as a Postdoctoral Fellow with the Broadband Communications Research Group, University of Waterloo. From August 2012 to July 2013, was a Visiting Scholar with the University of Waterloo and a Postdoctoral Fellow with Ryerson University. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Tennessee Tech University, USA. He is the author of more than 100 papers published in IEEE conferences and journals. His research interests include security and privacy-preserving schemes for smart grid communication networks, e-health, smart transportation, Blockchain, and machine learning. He received the NSERC-PDF award. He won the Best Paper Award from IEEE International Conference on Communications, Dresden, Germany, in 2009. He serves as an Associate Editor for IEEE INTERNET OF THINGS JOURNAL, and the *Peer-to-Peer Networking and Applications* (Springer). He served as a Technical Program Committee Member for several IEEE conferences and as a Reviewer for several journals and conferences, such as IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the *Peer-to-Peer Networking*.

MOHAMED ABDALLAH (Senior Member, IEEE) received the B.Sc. degree from Cairo University in 1996, and the M.Sc. and Ph.D. degrees from the University of Maryland at College Park in 2001 and 2006, respectively. From 2006 to 2016, he held academic and research positions with Cairo University and Texas A&M University at Qatar. He is currently a Founding Faculty Member with the Rank of Associate Professor with the College of Science and Engineering, Hamad Bin Khalifa University. He has published more than 150 journals and conferences and four book chapters, and co-invented four patents. His current research interests include wireless networks, wireless security, smart grids, optical wireless communication and blockchain applications for emerging networks. He is the recipient of the Research Fellow Excellence Award at Texas A&M University at Qatar in 2016, the best paper award in multiple IEEE conferences, including IEEE BlackSeaCom 2019 and the IEEE First Workshop on Smart Grid and Renewable Energy in 2015, and the Nortel Networks Industrial Fellowship for five consecutive years, 1999-2003. His professional activities include an Associate Editor for IEEE TRANSACTIONS ON COMMUNICATIONS and IEEE OPEN ACCESS JOURNAL OF COMMUNICATIONS, the Track Co-Chair of the IEEE VTC Fall 2019 conference, a Technical Program Chair of the 10th International Conference on Cognitive Radio Oriented Wireless Networks, and a technical program committee member of several major IEEE conferences.

WALEED ALASMARY (Senior Member, IEEE) received the B.Sc. degree (Hons.) in computer engineering from Umm Al-Qura University, Saudi Arabia, in 2005, the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Canada, in 2010, and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, Canada, in 2015. During his Ph.D. degree, he was a Visiting Research Scholar with the Network Research Laboratory, UCLA, in 2014. He was a Fulbright Visiting Scholar with the CSAIL Laboratory, MIT, from 2016 to 2017. He subsequently joined the College of Computer and Information Systems, Umm Al-Qura University, as an Assistant Professor of Computer Engineering, where he is currently an Associate Professor. His "Mobility impact on the IEEE 802.11p" article is among the most cited Ad Hoc Networks journal articles list from 2016 to 2018. His current research interests include machine learning-based and privacy-preserving smart systems. He is currently an Associate Editor for *Array*.