Security and Privacy Challenges in Connected Vehicular Cloud Computing

Arooj Masood, Demeke Shumeye Lakew, and Sungrae Cho

***Abstract*—Vehicular cloud computing (VCC) is an improvement from conventional cloud computing to new revolutionized computing services including intelligent transportation, autonomous driving and vehicle control, Internet browsing, online documentation, and infotainment. It enables vehicles to autonomously share heterogeneous computational resources while solving unanticipated critical problems dynamically. However, in a world of black hats, technology often has a dark side as well. Therefore, the VCC is limited by considerable security and privacy challenges. The special characteristics of VCC, including the multitenancy nature of clouds, intermittent wireless communications, high mobility of vehicles, and rapid resource elasticity with decentralized operations, have promoted security solutions used in vehicular ad hoc networks and conventional cloud computing to be revised. This paper first presents a state-of-the-art study of VCC that focuses on VCC architecture, its features analysis, and extensive VCC applications. Second, the proposed threats identification taxonomy and an exhaustive survey on security and privacy issues in VCC are presented under a layered approach: physical resource layer, vehicle-to-anything (V2X) network layer, and vehicular cloud layer, as well as at a complete system level. Finally, we highlight and discuss challenges and open research issues that can be considered as future research directions.**

Keywords*—Vehicular Cloud Computing, Security, Privacy, Security and Privacy.

I. Introduction

Modern technological innovations have revolutionized the ways in which vehicles are built, sold, and operated. Modern vehicles are pervasively computerized and connected. In other words, smart cars are being equipped with numerous embedded systems, such as electronic controlled units (ECUs), wireless-enabled on-board units (OBUs), trusted platform modules (TPMs), application units (AUs), and head units (HUs). Various ECUs, such as the engine control module (ECM), collect data on a vehicle's dynamics (e.g. speed and position information) and surroundings while controlling several subsystems of a connected vehicle. The ECUs collaborate by exchanging messages with an OBU and AU through an in-vehicular network. The AU is responsible for executing one or more applications provided by one or more remote service providers (RSPs). Each connected vehicle is also equipped with a TPM for storing cryptographic keys, certificates, and secure communications. In addition, vehicles are empowered by a variety of wireless access technologies (i.e., wireless access for vehicular environments (WAVE), which is based on the IEEE 802.11p standard) that enable vehicles to communicate with their surroundings [1], [2]. When considering such technologies, vehicles possess rich computing capabilities that make them ideal candidates for on-road mobile computing applications, including real-time sensing, computation, data relaying, and localization services.

According to recent statistics, there are more than one billion vehicles on roadways worldwide, and this figure is expected to increase to more than two billion by 2050 [3]. This growing number of vehicles has resulted in frequent traffic jams, driving problems, and road accidents and fatalities, which endanger human life. However, traffic jams and road fatalities can be limited by providing drivers with proper safety information on road conditions, surrounding environments, and critical driving situations, such as collision warning or active braking in a timely and secured manner. For this purpose, vehicles exchange safety information with nearby vehicles, road-side units (RSUs), and trusted third parties (TTP) through vehicle to anything (V2X) networks based on dedicated short-range communications (DSRC) technology. Exchanging non-safety information, such as location-based services, with RSPs can improve the travel comfort of drivers and passengers.

However, state-of-the-art vehicular services that provide web services over the Internet including intelligent transportation, autonomous driving, vehicular Internet browsing, online documentation, and in-vehicle infotainment can further enhance the driving experience. This creates a demand for on-board resource pooling [4], which permits distributed computing by exploiting the computing capabilities of vehicles. Traditionally, vehicular ad hoc networks (VANETs) are the wireless networking models that provide safety and non-safety services to vehicles. However, VANETs have their own unique characteristics, owing to the high mobility of vehicles, which present limitations on performance because of unreliable channel conditions [5]. Emerging vehicular applications require major architectural changes in VANETs, underlying the networking model that permits efficient and distributed computing. Therefore, a new service delivery model that combines VANET technology with cloud computing characteristics is required [6].

Vehicular cloud computing (VCC) is an emerging technology that revolutionizes network service provisioning by incorporating the characteristics of VANETs and cloud computing for on-demand self services [7]. VCC allows a group of VANET entities, such as vehicles and RSUs, within a certain range (approximately 300m) to autonomously share on-board resources and self-organize to form a cloud of large computing facilities. VCC manages on-board computing, communication,

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2018M1A3A3A02066018). *(Corresponding author: Sungrae Cho.)*

A. Masood, D. S. Lakew, and S. Cho are with the School of Computer Science and Engineering, Chung-Ang University, 156-756 Seoul, South Korea; (e-mail: arooj@uclab.re.kr; demeke@uclab.re.kr; srcho@cau.ac.kr)

TABLE I. ACRONYM AND DEFINITION

Acronym	Definition
AU	Application unit
CAN	Controller area network
CC	Cloud computing
CRL	Certificate revocation list
DSRC	Dedicated short range communication
DVC	Dynamic vehicular cloud
ECU	Electronic control unit
EVITA	E-Safety vehicle intrusion protected applications
GPS	Global positioning system
HoV	High occupancy vehicles
HU	Head unit
IaaS	Infrastructure as a service
IAM	Identity and access management
IoT	Internet of things
ITS	Intelligent transportation system
LBS	Location based service
LIN	Local interconnect network
LTE	Long term evolution
MAC	Message authentication code
MOST	Media oriented systems transport
OBU	On-board unit
PaaS	Platform as a service
RSU	Road side unit
RSP	Remote service provider
SaaS	Software as a service
SVC	Static vehicular cloud
TA	Trusted authority
TPM	Trusted platform module
TTP	Trusted third party
VANET	Vehicular ad hoc network
V2V	Vehicle to vehicle
V2I	Vehicle to infrastructure
V2X	Vehicle to anything
VC	Vehicular cloud
VCC	Vehicular cloud computing
VIN	Vehicle identification number
VM	Virtual machine
VMM	Virtual machine manager
VPKI	Vehicular public key infrastructure
WAVE	Wireless access for vehicular environment

sensing, and storage resources to balance resource limitations and service requirements. Because smart phones are considered the main clients of mobile cloud applications, these users are available in the vehicles. Congested passengers would like to perform office-related tasks while on the move, and fast moving vehicles would like to obtain upcoming traffic information on the road. Moreover, vehicles travelling with Internet access can jointly act as access points and provide broad networking access to the nearby vehicles travelling without Internet access. VCC is considered the key enabling technology that provides value added services to drivers and passengers.

However, the security and privacy of VCC is a critical requirement because legitimate users and attackers have equal privileges to share the same physical infrastructure [8], [9]. In most scenarios, attackers aim to alter the confidentiality, integrity, and availability of information on the cloud. The classic security and privacy problems related to standalone VANET [10] and mobile cloud computing environment are unchanged even if VCC technology merges both the VANET and mobile cloud computing environments [11]. However, there are several security and privacy challenges in VCC because of the autonomous and dynamic nature of vehicular clouds (VCs). A vehicle can dynamically join or leave the cloud at any moment, and there is no means of differentiating between a trusted vehicular resource and an attacker's resource. An attacker can masquerade as a legitimate cloud user and store malicious information on the cloud. Because VCC is based on the aggregation of shared resources, attackers can utilize system loopholes to obtain confidential information related to the vehicle or sensitive information. These attackers can tamper with the integrity of such information. An adversary may attempt to launch a denial-of-service (DoS) attack, such as jamming, to disrupt continuous cloud services or may attempt to inject malware to infect the credibility of the information on the cloud. There exists a potential risk of important information leakage, such as theft of details concerning vehicle identity and location information, from a vehicle's built-in sensors, while periodic cooperative awareness messages (CAMs) are broadcasted. Tracking vehicles on the move can be problematic in most cases. Even though pseudonyms and encryption techniques are used to secure vehicle identity [12], [13] and location information on the move [14], the absence of trust among cloud members produces considerable privacy concerns. Therefore, to exploit the advantages of VCC technology and to increase its adoption, these security and privacy issues must be addressed. The list of frequently used acronyms in this paper is provided in Table I.

A. *Motivation*

VCC has garnered significant attention in recent years as a special cloud computing platform capable of broadening network service provisioning in mobile computing. Different from traditional cloud computing, VCC exploits under utilized vehicular resources and dynamically allocate them to vehicles. Additionally, it can make rich application and services possible when neither Internet cloud nor road-side infrastructure is available. In particular, VCC allows a group of VANET entities such as vehicles and RSUs to autonomously share on-board resources and self-organize to form a cloud of large computing services. In addition to the applications provided by the conventional VANET, VCC provides support for real-world application including data outsourcing, outsourced computation (cloud-aided computing), data sharing and access control, and value-added services. However, achieving security and privacy in VCC is challenging due to the special characteristics of VCC such as multitenancy nature of clouds, seamless integration of resources, rapid resource elasticity with decentralized operations, in addition to the intermittent wireless communications and high mobility of vehicles, compared with conventional cloud computing and VANET. The main motivation of this survey is to provide a comprehensive survey of security and privacy issues in VCC together with the communication architecture and features, VCC application scenarios, threat identification and analysis, review of state-of-the-art mechanisms introduced to alleviate the security and privacy issues in VCC as well as to introduce important challenges and open research issues in designing security and privacy schemes for VCC.

TABLE II.
COMPARISON OF EXISTING SURVEY ARTICLES

Survey	**Architecture**	**Features**	**Applications**	**Security and Privacy Requirements**	**Threats Classification and Countermeasures**	**Comparative Study**
[15]	×	×	√	√	×	×
[16]	√	√	×	×	×	×
[17]	√	×	√	√	×	×
[18]	√	√	√	×	×	×
[19]	√	×	√	×	√	×
[20]	√	×	√	×	×	×
[21]	√	×	√	×	×	×
[22]	√	×	√	√ ×	×	×
[23]	×	×	√	×	×	×
Our survey	√	√	√	√	√	√

B. Related Work

There exist surveys on security issues in VANET in the literature including security and privacy requirements, attacks, and existing security solutions in VANET [11], [24]–[32], security and privacy challenges in vehicular named data networks [33], security and privacy issues in traffic management system and connected vehicles [34], [35], as well as security and privacy for innovative automotive applications [36]. However, the above survey works only focus on VANET security and privacy issues where research works proposed to address the security and privacy challenges of VCC are not considered.

Due to the unique features of VCC, in recent years, researchers from both industry and academia have investigated a variety of issues concerning VCC, including communication architecture and characteristics, application and services, simulators and testbeds, as well as security and privacy issues. Following these, a number of studies have been published to provide a review of VCC with various themes [15]–[23]. The themes of these research papers are summarized as follows. In [15], the authors presented a review on vehicular cloud applications and several issues on mobile vehicular cloud. [18] provided a survey focusing on VCC architecture, features, service taxonomy, and applications. In [16], a vehicular cloud taxonomy was presented with challenges involved in vehicular cloud architectural design and features. [17] surveyed vehicular cloud formation, vehicular cloud taxonomy, and vehicular cloud applications, and security and privacy issues. However, [16]–[18] lack in-depth analyses of the security and privacy issues that exist in each layer of the VCC architecture. In [19], a three-tier vehicular cloud networking (VCN) architecture was introduced by categorizing the clouds into categories of vehicular cloud, infrastructure cloud, and backend cloud. In addition, the authors proposed use cases in each cloud category and also highlighted security threats in VCN. In [20], a discussion on the role of VCC in road traffic management was presented along with a review of the VCC based traffic management solutions. Furthermore, a taxonomy of vehicular clouds was provided. [21] briefly discussed the differences between conventional cloud computing and mobile cloud computing. They provided an overview of VCC and studied the details of the architecture and services provided by the VCC. In addition they reviewed the recent research in VCC and presented future research challenges in terms of large-scale implementation, service reliability, and support for smart cities. In [22], the authors provided a comprehensive overview of cloud-based vehicular networks (CVNs) and proposed a conceptual hybrid cloud (HC) architecture. In addition, they presented open issues and challenges of communication reliability, accessibility, and quality of vehicle cloud services. [23] presented a discussion on the frameworks designed to utilize vehicles' on-board resources to provide vehicular cloud services. Further, they focused on detailed study of mobility generators, VANETs, and network simulators and available vehicle datasets. However, these articles lack discussions on related security and privacy requirements, threats, and countermeasures.

Unlike existing works, it can be seen that there still lacks a systematic survey paper that presents a comprehensive and detailed discussion on the security and privacy issues in a connected VCC environment. In a nutshell, the main contributions of our survey can be summarized as follows.

- We provide a review on state-of-the-art research issues on VCC architecture, features analysis, application scenarios, and an in depth analysis of security and privacy issues. To cover the broad aspects of security and privacy issues in VCC, we first recapitulate the diversified attack surface of connected VCC related to the technological developments from the perspective of in-vehicular network, V2X network, and vehicular cloud. Then, we address the security and privacy issues in VCC from a complete system perspective and with respect to the emerging applications in VCC.
- We propose threats identification taxonomy based on the detailed VCC architecture comprising of physical resource layer, V2X network layer, and vehicular cloud layer. Accordingly, we provide detailed security and privacy requirements, and identify potential security and privacy threats that can arise in a VCC system when security and privacy requirements are not met. In addition, we provide discussions on the research progress of security and privacy solutions.
- We point out and discuss challenges and open research issues that can be considered as future research directions.

To show the difference of our survey from existing works tailored to VCC, a comparison of research articles related to our survey is provided in Table. II. To the best of our knowledge, this is the first attempt to provide a comprehensive survey of VCC security and privacy issues together with communication architecture, features analysis, and application scenarios.

The remaining sections of this article are structured as follows. In Section II, we present a brief review of VCC architecture, features analysis, and application scenarios. Then, in Section III, we describe attacker model in VCC. Section IV presents the security and privacy issues in VCC in a layered approach. Physical resource layer attacks and countermeasures, V2X network layer attacks and countermeasures, and vehicular cloud layer attacks and countermeasures are provided in Sections V, VI, VII. In Sections VIII and IX, we present the discussions on security and privacy issues in VCC at a complete system level and emerging applications, respectively. Open issues and future research directions are presented in Section X. Section XI concludes the paper.

II. Vehicular Cloud Computing

With technological advances in vehicular networks, including automotive on board facilities and cloud computing, VCC technology has emerged as a promising solution to autonomous vehicular cloud of computing, sensing, communications, and the related use of considerable computational resources. This section provides a high level overview of the VCC architecture, features, and target applications.

A. Impact of Cloud Computing (CC) in the Automotive Domain

The concept of VCC was recently proposed to revolutionize vehicular networking models and resource utilization and support advanced vehicular applications in the automotive domain. The notion of cloud computing was introduced after the realization that instead of investing in expensive hardware, which is not fully always utilized, businesses can rent the required infrastructure, software, and services on demand from several infrastructure providers that have idle and under-utilized infrastructure and resources. A similar concept of on-demand delivery of IT resources and services has been envisioned for advanced automotive domains. As an increasing number of cars are equipped with on-board IT resources and several wireless access technologies, [4] proposed the integration of existing VANETs, sensing units, and on-board computing resources to create vehicular clouds while on the move. Because these on-board IT resources remain idle or under-utilized most of the time, these resources can be pooled dynamically to serve any authorized users, enable autonomy in resource sharing, and resolve critical unanticipated problems. In this context, interested drivers may find it useful to rent vehicular resources that are in excess to different users on demand to seek common advantages, as depicted in Fig. 1. In addition to presenting economically appealing solutions to large computing facilities, VCC is a promising solution for improving road safety and traffic management challenges in ITSs by providing flexible solutions to various traffic management services in real time (i.e., alternative routes, navigation, synchronization of traffic lights, etc.), which are desirable to various road safety actors, such as police, disaster management, and emergency services [6].

B. Vehicular Cloud Computing Architecture

Vehicles are characterized by high mobility, and vehicles can either be mobile or stationary at any given time. Therefore, vehicular resources can be pooled dynamically and autonomously. In addition to vehicles, several other entities such as RSUs, TSPs, and Internet cloud may be involved in VCC. In many scenarios, parked vehicles can be self-organized to additionally form an autonomous vehicular cloud. Mobile vehicles can autonomously create a vehicular cloud on the move by including other entities such as road-side infrastructure and/or Internet cloud as members of a vehicular cloud architecture. The autonomous and temporary nature of vehicular clouds has led to the emergence of a variety of VCC architectures. However, the design of a vehicular cloud architecture significantly depends on the objectives of cloud members, required functionality, application scenario, and service delivery model. Moreover, in a VCC architecture, the roles of vehicles may change according to the situations in which the vehicles are in [16]. Vehicles may act as resource providers, or as resource consumers of the cloud, or they may simultaneously act as both.

Owing to these dynamic characteristics of vehicular clouds, researchers proposed categorizing multi-objective vehicular clouds. For instance, [37] proposed a taxonomy on VANET cloud by dividing VANET clouds into three major architectural categories: VCs, VuCs, and HCs. In a VC architecture, vehicles serve as service providers of cloud services and form a dynamic cloud via direct V2V communication to solve real-time traffic problems. In the architecture of VuC, vehicles act as service consumers and indirectly use cloud services on the move

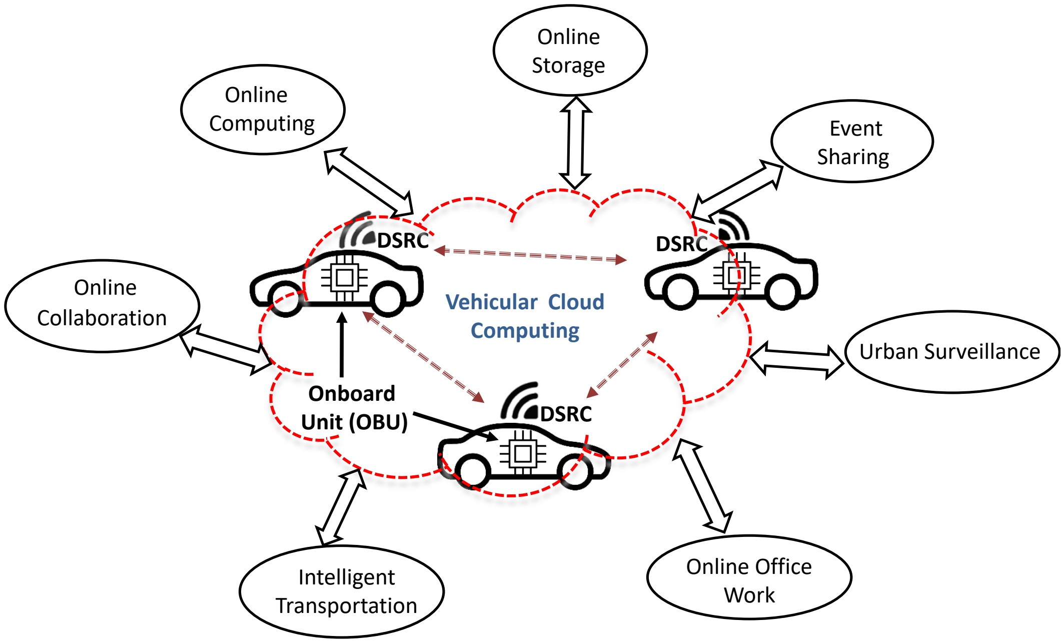

Fig. 1. Impact of cloud computing in automotive domain

TABLE III. VEHICULAR CLOUDS TAXONOMY

Reference	Cloud types	Description
[37]	VC, VuC, HC	VC: vehicles serve as service providers using V2V communications VuC: vehicles act as resource consumers using V2I communications HC: vehicles simultaneously act as service providers and service consumers via both V2V and V2I communications
[38]	VTC, VAC, VWC	VTC: vehicles access cloud services directly using road-side infrastructure VAC: vehicles provide cloud services by connecting to other vehicles directly VWC: vehicles simultaneously serve as resource providers and service consumers
[39]	General VCA and specific VCA	General VCA: architecture based on various cloud service types Specific VCA: architecture based on specific cloud service types

through V2I communication. Vehicles in HC architecture act as both service providers and service consumers through the simultaneous combination of the VC and VuC architectures. [38] proposed another taxonomy for context aware vehicular clouds. The taxonomy consisted of three architecture types: VTC, VAC, and VWC. Vehicles access cloud services on the move using the gateway deployed as road-side infrastructure and act as resource consumers in the VTC architecture. In a VAC architecture, connected vehicles selectively allocate their computing resources to other vehicles by functioning as resource providers. In the VWC architecture, vehicles simultaneously serve as infrastructure providers and end users. In [39], the authors provided detailed overview on proposed VCAs and proposed a VCA taxonomy based on the service type of the architecture. The taxonomy is divided into two main categories: general VCA and specific VCA. In general VCA, the design of the architecture is based on different cloud applications and requirements. However, general VCAs usually comprise three layers: device, communication, and service. Specific VCAs incorporate different concepts as they focus on solving different problems, such as traffic, routing, disaster management, and vehicle monitoring. Table. III summarizes the different vehicular cloud taxonomies presented in the literature.

In this section, we provide a high level architecture of VCC that consists of two main domains: 1) V2V VCC and 2) infrastructure-supported VCC. Fig. 2 illustrates a general VCC architecture.

1) Vehicle-to-Vehicle Cloud Computing: Several vehicles can cooperate to form an autonomous cloud by relying solely on their own on-board resources to utilize low-sized road-side applications, such as safe driving and traffic management. In addition, the on-board resources can be leased for complex and high-bandwidth applications, such as video gaming, online document processing and publishing, and social networking.

2) Infrastructure-Supported VCC: The emergence of enabling wireless access technologies in vehicles and road-side infrastructures that use communication technologies, such as access points, cellular base stations, and vision technologies, such as smart wireless cameras, provides vehicles and traffic management authorities with information concerning traffic conditions and events on the road. Traffic management authorities can exploit this information to dynamically schedule and manage traffic accordingly. Because vehicles in parking areas are temporarily immobile, a vehicular cloud developed at a parking area has additional advantages in terms of storage and computation provisioning [19].

In addition, vehicular clouds may benefit from the Internet

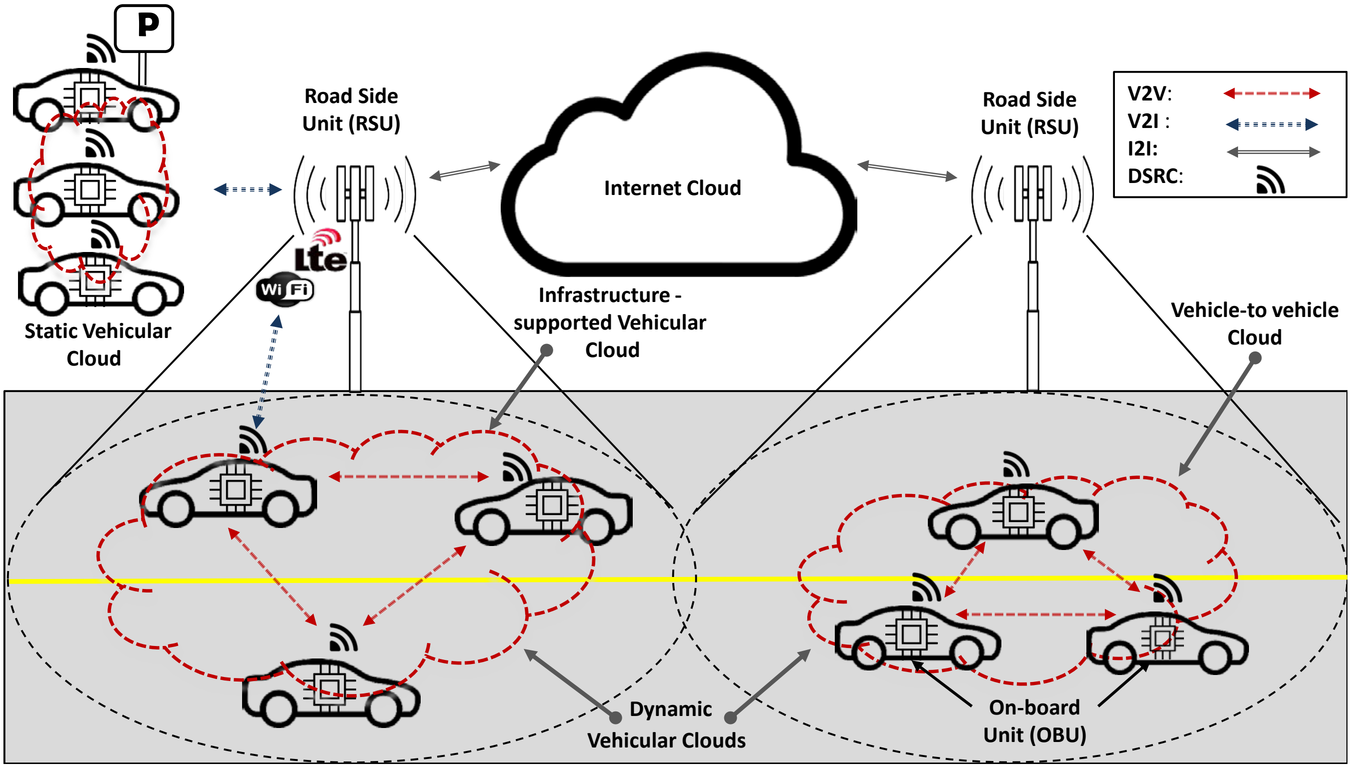

Fig. 2. Vehicular cloud computing architecture

cloud using existing static infrastructure. The interaction of vehicular clouds with the Internet cloud provides additional computing capabilities and real time services to vehicular users, thereby enriching the VCC environment. With VCC, Internet cloud services can be accessed from any location.

Both the V2V cloud computing and infrastructure-supported VCC architectures can be deployed based on either a DVC model or an SVC model. A DVC is applied to mobile and dynamically changing vehicular cloud vehicles. For instance, vehicles moving on roads and highways can develop a DVC with or without infrastructure support. A vehicle may join the DVC or leave it at any moment. Moreover, owing to the high mobility of vehicular vehicles and the dynamic nature of DVCs, the time interval of a vehicle joining or leaving the vehicular cloud is relatively short allowing measured services with a short-lived cloud. SVCs are deployed with the participation of stationary vehicles parked on the road or at various parking lots, with or without infrastructure support. In the SVC deployment model, vehicular resources are shared and rented out to various customers on demand, which is quite similar to conventional cloud resources being virtualized and rented out to various users on demand. For instance, an SVC can be realized at shopping malls or parking plazas, where many people park their cars for 2 to 3 hours, while shopping [40]. Mall authorities can utilize idle computing resources and develop an SVC of parked vehicles. Mall authorities can delegate some of the routine computational tasks to this SVC datacenter while providing free Internet service to mall customers through the VC.

C. *Features Analysis*

VCC includes distinguishable features that make it different from existing cloud computing technologies. The use of flexible and dynamic vehicular resources will allow drivers and vehicular users to run vehicular applications on the go without being concerned about limited computing resources.

1) Autonomy: To alleviate the computing burden on vehicles, VCC allows autonomous cooperation of vehicular computing resources into VCs. In this regard, VCC improves resource utilization on vehicles and is able to solve complex computing tasks that cannot be solved by a single vehicle. However, sharing onboard resources among untrustworthy and unfamiliar vehicles lead to several security and privacy challenges. Since vehicles are owned by different individuals, vehicular resources in VCs cannot assumed to be trustful or honest-but-curious [4].

2) Mobility and Dynamicity: VCC exploits underutilized vehicular resources and dynamically allocates them to vehicles without requiring an early planning of resource provisioning. Moreover, mobility of vehicles allows onboard resources to be utilized in areas with restricted access to the Internet. However, high mobility of vehicles in VCC causes frequent disconnections and rapidly changing onboard resources in the VC since fast moving vehicles may form various VCs with different vehicles at different locations. Thus, identity authentication of highly mobile vehicles and the management of vehicles' authentication credentials becomes extremely difficult [41], [42].

3) Decentralized operations with elastic resources: In VCC, the demands of additional resources can be fulfilled easily because of the elastic resource expansion feature of VCs. This feature allows VCs to operate in a decentralized way and allows them to function without central cloud management. However, when vehicles are allowed to share on-board resources autonomously, attackers can share an equal opportunity to become part of a VC. For instance, an attacker may pretend to be a legitimate user requesting a service and get unauthorized access to the cloud resources or sensitive data that they normally do not have an access to, or they can maliciously utilize the cloud resources [43].

4) Resilience: VCC operates on two different communication modes facilitated by V2V or V2I. This implies that the services provided by VCC can still be reliable even if neither the Internet cloud nor roadside infrastructure is accessible. Because of the vehicles connectivity through a shared wireless medium, an attacker may threaten the availability of communications channel to disrupt the ongoing VCC services [18], [43].

5) Localization: Most applications in VCC rely on location information to create connections and share local data such as cooperative driving, emergency events, crowdsensing, and traffic status reports. However, some malicious vehicles may share untruthful location data resulting in serious consequences. For instance, vehicles in a VC may ask for advice on route planning and untruthful location information may lead to unfamiliar locations and put them in danger. In addition, attackers may catch private information about vehicles and threaten the location privacy of vehicle owners since a vehicle's information and identity are pinned to its owner's identity. Therefore, the security and privacy of location information should be provided in VCC [17].

6) Heterogeneity: VCC includes vehicles with heterogeneous ECUs manufactured by various automotive companies that possess various capabilities such as speed of processor, storage capacity, volume of memory, and CPU power. Interoperability of various OBUs and coordination of their resources provides all the advantages introduced by VCC, which is a marked feature of VCC. However, securing these heterogeneous on-board resources is difficult because most cryptographic algorithms require complex computations, and OBUs are expected to meet certain hardware conditions. In addition, the ECUs are connected via the heterogeneous internal buses and are exposed to one another, constituting an in-vehicle network attack surface. The connected ECUs are also externally accessible through a wide variety of I/O interfaces constituting an external attack surface of vehicles [18], [43], [44].

7) Seamless Integration of Resources: VCC logically integrates the computing resources of vehicles into VCs and provides it to the vehicles that require more computing resources. Since VCC allows potentially malicious vehicles with underutilized resources to provide services to other vehicles in a VC, it raises security challenges such as computing security and data security [43].

D. VCC Application Scenarios

In this subsection, we list several application scenarios for VCC based on the distinctive features of VCC technology and discuss accordingly. Vehicular resources can be pooled autonomously and dynamically while vehicles drive on roads and highways. Similarly, VCs can also be formed while vehicles are parked in streets or in large parking lots for both long and short durations. Thus, based on the VCC deployment model, VCC application use cases can be categorized in DVCs (such as road and driver safety, autonomous driving, infotainment and comfort, traffic management, and managing evacuation), SVCs (such as data center at parking, augmenting fog computing, and vehicular cloud content caching), or in both scenarios (such as outsourced computing, data sharing and access control, data outsourcing, and value-added services).

DVCs are formed dynamically while vehicles drive on roads and highways. Because of a large number of moving vehicles and dynamically changing traffic conditions on our roads and highways, static solutions of managing and controlling traffic flows are neither useful nor efficient. Therefore, managing traffic flows in real-time can be a complex problem. Although a number of research efforts have been made in the past to address the problem of traffic management in the context of ITS and VANETs, such efforts have not been efficient in reporting real-time traffic conditions, i.e., congestion to the relevant authorities and have not been able to provide a dynamic solution that mitigates such problems in real-time. In this context, vehicles on the move can self-organize to form an autonomous cloud which effectively solves the critical congestion problem in real-time. VC application scenarios that exploit DVCs such as road and driver safety are generally supported by V2V cloud computing while application scenarios such as infotainment and comfort, traffic management, and managing evacuation can be realized through infrastructure-supported VCC.

Following this, we provide a detailed description of such emerging application scenarios based on a dynamic vehicular cloud deployment architecture.

(i) Road and Driver Safety: Road safety applications represent the most important class of VC applications. A VC can be formed when a vehicles' sensor requests neighboring vehicles to form a large wireless sensor network for improving fidelity and ensuring high-accuracy information on road hazards, traffic conditions, speed breaker, and specific events i.e., accidents. The sensing data collected from neighboring vehicle can be integrated to form a real-time picture of road conditions for safe driving. Unfortunately, attackers can easily become part of the VC and broadcast forged messages into the transportation system. Several unexpected situations may occur due to these security issues. Therefore, it is important to provide controlled access of messages in VCC.

(ii) Autonomous Driving: Autonomous driving is also known as automated driving and is heavily reliant on automated sensors and driving functions [45]. VCC enable vehicles to self-organize and integrate OBUs to provide an automated self-driving environment whereby sensors can detect obstacles on the road with high-accuracy, high-definition cameras can spot road hazards in real time, and global navigation satellite systems can provide highly accurate information on the positions of vehicles. However, autonomous driving is vulnerable to several security threats since automated OBUs are the target of attackers. A vehicle with malfunction component can disseminate incorrect information. Camera (blind) and GPS spoofing are two main security problems in automated driving [46], [47].

(iii) Infotainment and Comfort: These aim at enhancing the travel experience of drivers by providing advanced vehicular applications through infrastructure-supported VCs since these applications are generally offered by trusted RSPs where the VC communicates with RSPs using infrastructure-supported communications (4G/LTE). However, a rogue RSP may pretend to be a valid service provider and delivers untruthful data and learn sensitive information from vehicles. The attacker may also try to attract clients by providing reliable service first and then it may try to gain unauthorized information for its own benefits.

(iv) Traffic Management: V2X entities, i.e., vehicular sensors, road-side infrastructure, and road-side sensors, can form VC in which vehicles collaborate to collect, analyze and process traffic data. The processed data can then be immediately used by drivers to enhance the management of traffic flows in real-time and to enable cooperative navigation services among drivers. Moreover, this data can also be provided to traffic management authorities for performing advanced spatio-temporal traffic analysis, optimizing traffic signals, and dynamically managing traffic lights [48]. However, a compromised vehicle may deliver untruthful data about road conditions or forge identities to provide multiple sensing data.

(v) Managing Evacuation: In case of emergency evacuations and predicted disasters such as hurricanes, traffic authorities often perform simulations to identify traffic control strategies. However, it puts a large burden on traffic management authorities. VCs can facilitate evacuation before disaster strikes; therefore we assume network connections are available. Vehicles can self-organize into one or more inter-operating VCs and collaborate with emergency centers for successful evacuation. VCs perform computations to dynamically manage traffic flows and determine the direction and speed in which traffic is flowing and provide services to vehicles reliably, even when neither the RSU nor cloud is available when the signal coverage is poor. For example, VCs can regulate traffic for the evacuation on highways and manage traffic flows on local roads. However, in order to determine a suitable route for evacuation, vehicles need to perform simulations. Since vehicles in a VC belong to different individuals. It is reasonable to suspect computation results returned by the vehicles. An attacker vehicle may return an arbitrary computation results.

In static vehicular clouds (SVCs), vehicles can group into VCs when stationary and possess the same behaviour as that of a conventional Internet cloud. In such situations, on-board resources are available but idle, and the opportunity for utilizing such resources has been exploited in many works [49], [50], [51]. This provides a means for SVC computing where vehicles can combine to form one or more static VCs by accumulating storage capacity and computing power of the participating vehicles and serving as distributed data centers for real-time information processing. Following this, we provide a detailed description of emerging application scenarios based on a SVC deployment architecture.

(i) Data Center at Parking: In urban settings, parking lots are attractive examples for car pooling. Vehicular computing resources are idle for a long period of time and can be used to form a computer cluster of huge storage. This scenario provides an attractive opportunity for businesses to the idle vehicular computational resources in parking lots as potential computing facilities. For example, a small company can employee a few hundred people. Their vehicles remain parked in the car park area. Everyday, the computing resources in those vehicles are sitting idle. The company can provide an incentive to employees who rent resources to provide various types of services. Meanwhile, it provides an opportunity to an attacker to break the location privacy of users or identify users. For instance, an employer could perform traffic analysis by eavesdropping vehicular communications on the company parking lot, and after distinguishing which identifier belongs to which vehicle, the employer can automatically collect arrival and departure times of employees.

(ii) Augmenting Fog Computing Services: Fog services including computation, storage, and networking are hosted at the edge of wireless networks and tend to provide reliable access to delay-sensitive mobile applications. However, in certain cases, fog computing resources may be insufficient because of the large quantities of data generated from various mobile and Internet of Things (IoT) devices, leading to acute performance degradation. This problem can be alleviated by supplementary unused VC resources while vehicles are stationary [51]. Fog computing services are provided by fog nodes which are managed by the trusted entities, i.e., cloud. However, vehicles cannot be assumed honest or truthful since they are owned by different individuals. Because of this different level of trust, malicious vehicles may be interested in private information or may even launch active attacks to influence the fog computing service results.

(iii) Vehicular Cloud Content Caching: Many state-of-the-art networking technologies, such as caching popular contents at the edge of the network, e.g., small base stations (SBSs) alleviates the network burden of core cellular networks. However, their performance is limited because they heavily rely on a fixed infrastructure. In this context, caching at the VC can bring contents closer to users. By caching popular contents at the vehicular clouds, duplicated requests for cached contents could be largely reduced at the core cellular network since the cached contents can be directly relayed to requesting users using V2V and V2I communications. However, a malicious vehicle may try to gain unauthorized access to the caching data for its own purposes.

On the other hand, VCC can be exploited in various other real world applications such as outsourced computing, data outsourcing, data sharing and access control as well as value-added services either in dynamic or static cloud deployment model [52]–[55]. Following this, we provide a detailed description of these emerging application scenarios.

(i) Outsourced Computing: To alleviate the computing burden on vehicles, VCC logically integrates on-board computing resources and provides to vehicles that require those computing resources. VCC allows vehicles to outsource the massive computations to a group of vehicles in a VC while executing simple computation tasks. Since vehicles belong to different individuals, due to the different levels of trust, vehicles may be interested in the result of outsourced computations, or they may also return an arbitrary computation result to save their own computations leading to arbitrary results attack. Moreover, before performing computations, vehicles may be interested in intercepting the sensitive outsourced data leading to data interception attack. In addition, internal attackers can launch active attacks on the computations to tamper with the integrity of outsourced task [52]. Thus, it is required to identify the trustworthy vehicles to form a VC, protect the input and output of the outsourced computing, and verify the integrity of the outsourced computing results.

(ii) Data Outsourcing: VCC provides various services to the road users such as vehicular crowdsensing. Vehicular crowdsensing allows vehicles to cooperatively collect and share data about the environment, which is well beyond the capabilities of the RSUs. However, the sensing data may be susceptible to errors and background noise. Thus, in order to obtain accurate sensing data, extensive research efforts have been made in vehicular crowdsensing [56], [57]. However, the challenges of security and privacy have not been addressed. For instance, attackers can launch badmouth attacks by providing untruthful data. Moreover, attackers can perform on-off attacks in which attackers may behave honestly in the start but start to launch attacks when they have obtained high trust values. Thus, in data outsourcing, it is required to obtain truthful data, provide reliable trust management, ensure privacy, and segregate malicious vehicles from legitimate vehicles.

(iii) Data Sharing and Access Control: VCC enables resource management of on-board resources to balance the resource limitation and service requirements of vehicles. Congested passengers would like to perform office-related work while on the move. To this end, sensitive data such as documents, files, or codes are shared among vehicles. However, attackers can easily become part of VC and may tamper with the integrity of sensitive data. Specifically, data privacy attack, data integrity attack, and anonymity attack are major security and privacy concerns for data sharing applications. In order to securely share data among vehicles, attribute-based encryption (ABE) can be employed to achieve access control on data [54]. However, ABE-based encryption involves computation intensive operations, which cannot be performed on resource-constrained on-board unit. To this end, computationally complicated ABE-based encryption and decryption tasks can be performed by utilizing shared pool of computing resources in VCC together with Internet cloud.

(iv) Value-added Services: VCC improves resource utilization on vehicles and is able to provide highly diverse services for vehicular users, i.e., value-added services with minimum help from the Internet cloud. Such value-added services include virtual reality, massive multiplayer online games, map downloads, as well as other new vehicular services to enhance travel pleasure of vehicle users and are supported by several cloud service providers (CSPs). However, a vehicle may need to switch and choose services among several service providers. Thus, it is required to ensure mutual authentication and key agreement between various service providers and vehicle, untraceability and unlinkability of vehicles, and to segregate malicious vehicles from legitimate vehicles.

III. Attacker Model in VCC

VCC includes distinguishable features that make it different from existing VANETs and cloud computing technologies. In this section, we provide attacker model in VCC based on its distinguished features.

One of the characteristics that distinguishes VCC from CC is the dynamically changing amount of computing resources. The short-term interaction of vehicles and frequently changing set of on-board resources increase trust issues among vehicles because each vehicle will meet frequently changing neighbors, many of whom it has never met before and is unlikely to meet again. In addition, VCC may allow potentially malicious vehicles with underutilized resources to provide services to others. This feature brings new security and privacy challenges such as data security and computing resources. VCC is expected to achieve its full potential if it offers decentralized management and seamless integration of the on-board computing resources of participating vehicles. However, it provides an opportunity to attackers to exploit system loopholes and achieve their adversarial targets. Since vehicles in a VC communicate through intermittently short range wireless communications, they experience frequent wireless transmission impairments, bringing significant security and privacy challenges to the VCC system such as authentication management, authorization control, trust relationship, and accountability issues.

Unlike VANET, the multitenancy feature of VCC, which refers to the cloud characteristic of sharing multiple computing resources with multiple users at the same time, makes security model implementation in the VCC environment more challenging. In addition, the heterogeneous and dynamic on-board computational, sensing, and storage resources lead us to anticipate the discovery of numerous security and privacy challenges informed through conventional wireless networks, VANETs, or

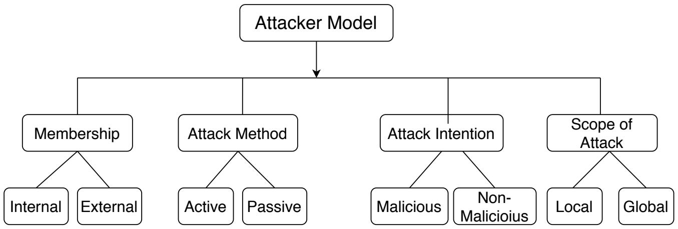

Fig. 3. Attacker model in VCC

CC. However, several security issues are inherently transferred to the VCC system through the integration of related technologies such as VANET, wireless communications, and CC.

Conventional cloud computing models can achieve a desired level of security of cloud assets by preventing attackers from accessing a cloud system [58]. However, in a VCC environment, in addition to normal users, attackers can easily become the participants of VC, making the VCC system more vulnerable to security and privacy threats. An attacker, who is a participant of VC can utilize the shared system loopholes to achieve their targets of stealing confidential information related to identity and location of the target vehicle and perform tracking of the vehicle or tamper with the integrity of real and imminent road safety information exchanged among active VC members and reported to the cloud for assisting future cloud members.

Owing to such distinguished characteristics of VCs, an attacker has the opportunity to become an equal part of the vehicular cloud and share a part of the same physical machine, including CPU, memory, data, programs, and networks to achieve its target. Although users are isolated at virtual levels and are assigned different virtual machines in a VC, the underlying hardware is not separated. These potential vulnerabilities provide an interesting platform to a number of attackers to join the cloud and achieve their adversarial objectives. Thus, various types of attackers are likely to become part of a VCC system and can be categorized according to four bipolar criteria: active vs. passive, internal vs. external, malicious vs. non-malicious, and local vs. global [59], [60]. A bipolar criteria states that an attacker involves attack capabilities from the four categories mentioned above and as illustrated in Fig. 3. Thus, the details of attackers can be summarized as follows:

1) Internal vs. External: Attackers can be distinguished on whether they are members of VC or not. An *internal* attacker has authorized access to the VC and can communicate with other cloud members. An *external* attacker does not have authorized access to the VC. Instead, they perform attack by means of physical intrusion, or a connected network [61]. For example, an external attacker may directly harm the static infrastructure, i.e., an RSU physically on the road. We assume that an external attacker can eavesdrop on wireless communications.

2) Active vs. passive: Attackers can actively change status of VC or remain passive. An *active* attacker can actively inject messages, or modify the contents, resources, and signals to directly inflict damage on the VC. An active attacker tampers with the integrity of the stored information on the cloud. This information may include sensitive data, important documents, executable code, and results. Tampering with the integrity of information will cause deception in two ways: 1) modifying the contents so that a user relies on the modified version of data, and takes its next action based on the modified information, and 2) a user accepts the modified information to be authentic and releases this information to other VC users. A *passive* attacker cannot inject or modify messages but can eavesdrop on the wireless channel and collect pseudonyms at every intersection where they have deployed their eavesdropping station [62].

3) Malicious vs. Non-malicious: A *malicious* attacker does not seek personal benefits in attacking the VCC system. A malicious attacker intends to disrupt the normal functioning of VCC or harm VCC entities (e.g., OBUs, RSUs) by introducing malware. In contrast, a *non-malicious* attacker is very precise in terms of its attack targets [63]. For example, an attacker may pose as an emergency vehicle and cheat other vehicles in to lowering their travelling speeds.

4) Local vs. Global: This category defines the range of attack of an attacker. A *local* attacker is limited in range of attack and can only access to the nearby vehicles and infrastructure. For example, an attacker can target to deploy a limited number of eavesdropping stations only at the road intersections to cover a large area for detecting vehicles entering and exiting from the intersections [64]. A *global* attacker can have a broader scope of attack by expanding their range and controlling several VCC entities across the network and possesses global knowledge of the vehicular cloud network [62]. Based on this model, a global passive attacker (GPA) who can be internal or external, can eavesdrop on vehicle broadcasts and break the location privacy of VCC users in their region of interest [65]. A GPA can leverage the existing infrastructure (e.g., RSUs) and deploy its own eavesdropping stations (e.g., RSUs) to estimate the locations of vehicles in their area of interest.

Compared to a GPA, a local passive attacker (LPA) can only utilize the existing infrastructure for eavesdropping broadcasts and estimating locations of the vehicles. Therefore, the region over which an LPA can eavesdrop is limited and depends on the distance between successive RSUs and vehicle's transmission speed. An EMA can illegally access an RSU in a V2I based VCC and introduce malware, or it can harm the RSU physically on the road, thereby preventing the RSU from participating in VCC services. Compared to an EMA, an internal malicious attacker (IMA) can infiltrate any on-board unit by introducing malware and leverage this ability to control a wide range of automotive functions and disrupt the normal functioning of VCC.

IV. Security and Privacy Issues in VCC - A Layered Approach

In this section, we provide details on various security and privacy aspects in VCC. Specifically, we provide details on security and privacy requirements and threats identification. VCC security and privacy requirements define the requirements that should be taken into consideration when developing a VCC architecture. Inability to fulfil these requirements may lead to

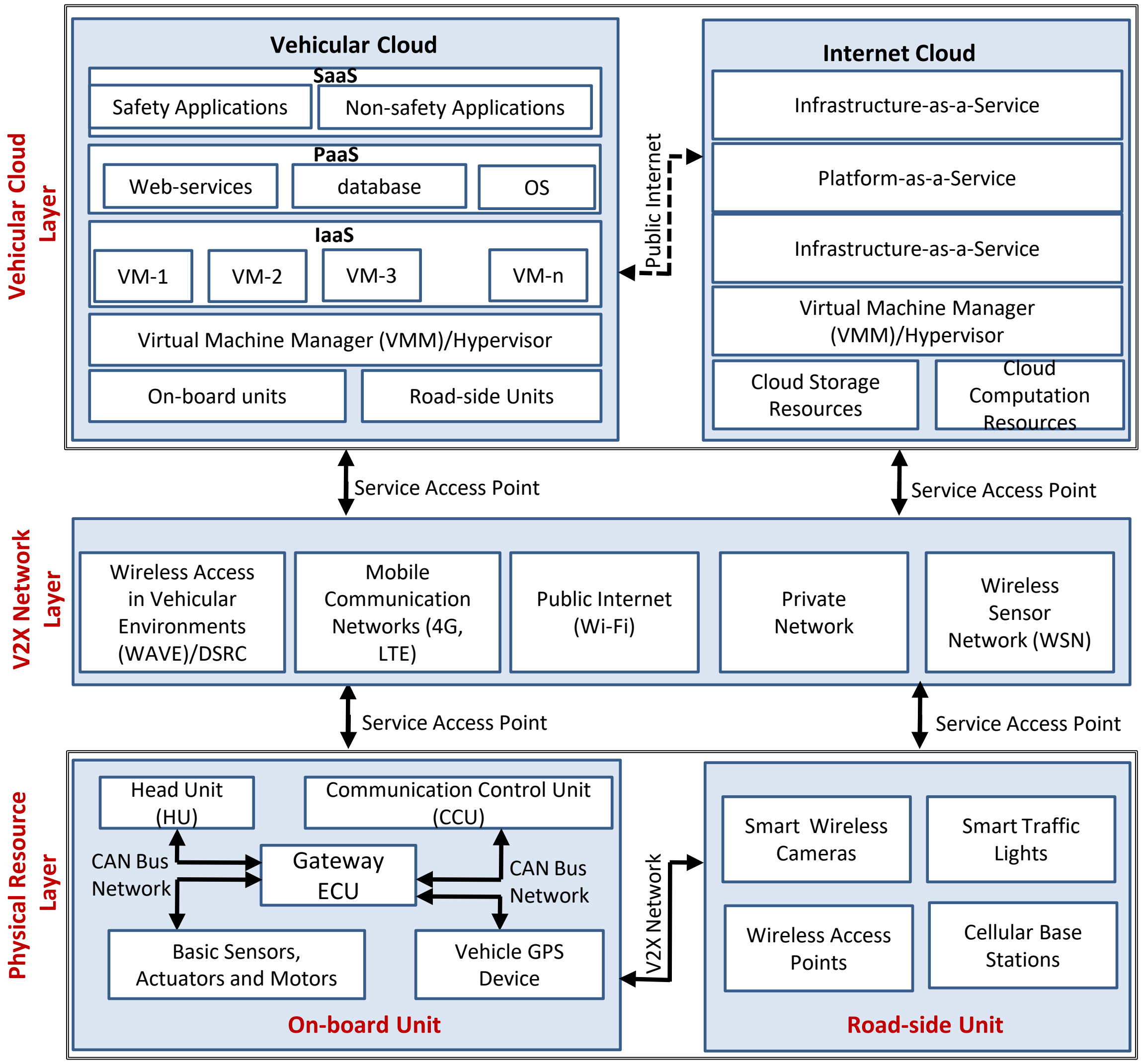

Fig. 4. VCC architectural components

possible security and privacy threats in VCC. Accordingly, We provide our proposed taxonomy of threats identification in VCC. Particularly, Section IV-A provides details on the security and privacy requirements in VCC based on separate resource layers provided in the VCC architectural components as shown in Fig. 4. While, Section IV-B presents security and privacy taxonomy proposed in this paper based on the security vulnerabilities found in each resource layer of VCC.

A. *Security and Privacy Requirements*

Security and privacy are considered as the most important requirements for VCC because of the sharing of private data and computing resources on the cloud and security perceptive nature of vehicular applications. Understanding and clearly defining fundamental security and privacy requirements is imperative to determining security perceptive solutions that lead to secured VCC systems. To identify the detailed security and privacy issues in VCC, VCC architecture illustrated in Fig. 2 is further decomposed. The detailed VCC architectural components (see Fig. 4) comprises three tightly-coupled layers: 1) *physical resource layer*, 2) *V2X network layer*, and 3) *vehicular cloud layer*. The physical resource layer consists of various OBUs and sensors that are interconnected via an in-vehicle interconnect CAN/FlexRay bus that control the vehicles' subsystems. The V2X network layer consists of wireless V2V and V2I access technologies for accessing VC applications. The VC layer enabled by virtualization technology pools under-utilized on-board vehicular resources of dynamically moving autonomous vehicles on the move to create a VC. In a VC, pooled on-board resources such as sensors, storage, computation, and communications, are dynamically allocated to authorized users on demand. However, the vehicular cloud layer can (or cannot) be connected with the Internet cloud layer to provide additional services to users. Each of these layers constitutes a potential security attack surface and contributes to the security and privacy compromization of VCC system.

Significant research efforts have been actively dedicated to V2X communications security [28], [63], [66], [67] and cloud computing security issues [68]–[71]. However, addressing security issues and protection of internal automotive subsystems such as on-board architectures and in-vehicle network has long been an overlooked area of research. This paper argues that a comprehensive analysis of VCC security and privacy issues must go beyond V2X-centric security solutions and, in particular, must provide mechanisms for secure data transmission and reception in vehicles' internal subsystems.

1) Physical Resource Layer: In modern automobiles, state-of-the-art vehicular OBUs can contain upto 80 ECUs that are connected through heterogeneous bus network technologies, such as CAN, local interconnect network (LIN), FlexRay, and media oriented systems transport (MOST) [72], [73]. Although every bit of information transferred through these network media could be critical to the driver's safety, security and privacy mechanism has unfortunately has not been considered during the design of in-vehicle communication protocols. As the most widely used in-vehicle network media, CAN-bus has become the *de facto* standard in the automotive domain because it ensures higher data transmission reliability and reduces the complexity of communication lines [74], [75]. Fig. 5 illustrates an analogy to an in-vehicle network. However, the CAN protocol does not ensure the confidentiality and authenticity of CAN frames, enabling adversaries to eavesdrop on the CAN frames and conduct replay attacks [76], [77]. Owing to such vulnerabilities, in-vehicular network security must be considered as a baseline and paramount to securing the VCC system. [78] presented security requirements of engineering processes for automotive on-board networks and described a process for identifying and prioritizing such requirements. The security requirements engineering process begins by defining the use cases of automotive on-board networks (e.g., V2V communication, V2I communication, use of nomadic devices such as USB, and workshop diagnosis) that are based on wireless communication technologies. An investigation of the security threat scenarios (structured using attack trees [79]) is then performed and an assessment of the relevant risks associated with those threats is made. Security requirements include authenticity, i.e., 1) information originating from inside the vehicle's sensors should be authentic in terms of source, content, and time, and 2) information received by a vehicle from another vehicle should be authentic in terms of source, content, and time. The security requirements and security mechanisms inside the vehicle and on the wireless communication channel must guarantee the authenticity and integrity of information originating from a source and received by the destination vehicle.

In this regard, the E-safety vehicle intrusion protected applications (EVITA) project [80] performs threat and risk analysis of the on-board security architecture (in-vehicle hardware and software) and identifies the following key security requirements:

(i) Integrity of Trusted Hardware Security Module: Tampering with the stored cryptographic keys and operations inside the trusted hardware module, such as TPM, must be prevented to secure cryptographic operations.

(ii) Integrity and Authenticity of In-vehicle Software and Data: Unauthorized software updates, and unauthorized alteration of locally stored data on the OBUs must be prevented or at least the authenticity of the claimed user for software updates or data modification must be determined.

(iii) Integrity and Authenticity of In-vehicular Communication: Authenticity of the sender OBU and unauthorized modification of the message and data, which is sent over the in-vehicle network, must be detectable and verifiable by the receiver OBU.

(iv) Confidentiality of In-vehicular Communication and Data: Because in-vehicle networks are broadcast communication networks, authorized disclosure of broadcast messages and data must be prevented. Safety messages and confidential data must only be intelligible to the authorized OBU.

(v) Proof of Platform Integrity and Authenticity to Other Vehicles: An entity inside an in-vehicle platform must be capable of proving the integrity and authenticity of its internal hardware and software configurations and data sent to other vehicles.

2) V2X Network Layer: Because wireless networks include ”glue” sticking cloud users, vehicular applications and resources in a vehicular cloud use V2V and V2I communications. V2V- and V2I-based communications rely heavily on a shared wireless communications channel with multitenancy challenges. Owing to such challenges, several security threats can affect communications and lead to network disruption. The security and privacy requirements such as availability, data confidentiality, data integrity, authentication, authorization, privacy and anonymity, non-repudiation, and traceability and revocation are used to measure the security and privacy of V2V and V2I communications [66], [81].

(i) Availability: The availability requirement ensures that the wireless communications channel is available, and the wireless network is in a functioning state. Users can process and exchange information over the wireless communications channel in real-time.

(ii) Data Confidentiality: The confidentiality requirement guarantees that exchanged information are encrypted properly and accessible only to authorized and designated recipients [11], [82].

(iii) Data Integrity: Data integrity ensures that stored data and exchanged safety messages are protected from unauthorized modification on the wireless communication channel, and OBUs can verify and validate the integrity of the received data and messages to ensure authenticity.

(iv) Authentication: Authentication is one of the most important security measures used to prevent various attacks on the wireless communications channel from malicious entities in the network. It requires source authentication to ensure that messages were generated and sent by

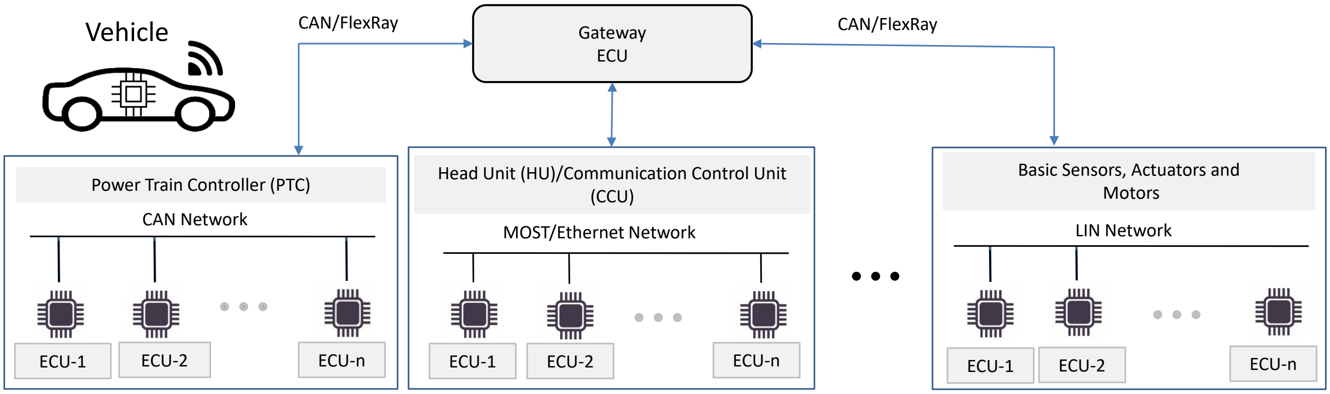

Fig. 5. In-vehicle interconnection network

legitimate users and location authentication to ensure the integrity and relevance of the received information.

(v) Key Agreement: After a successful authentication, vehicles and service providers can share a session key for encrypting and decrypting the subsequent communications to achieve confidentiality and integrity of the transmitted data [31].

(vi) Privacy and Anonymity: Privacy is the protection of a vehicles' credentials, such as the vehicles' identity and location information. Personal information should not be identifiable on a wireless communication channel, and the access rights of the driver's personal data should be controlled.

(vii) Authorization: It is necessary to define access control and authorization mechanisms properly and separately for various cloud entities. Specific rules should be enforced for allowing access to the data or denying specific cloud entities access and/or use of certain data or resources.

(viii) Non-repudiation: Non-repudiation is a security service that ensures that the sending and receiving parties of the data cannot deny its transmission and reception on the wireless communications channel in case of any conflict. Each VCC entity should be uniquely identifiable for its data and actions to achieve source and data authenticity.

(ix) Traceability and Revocation: Transportation authorities must track malicious network entities to remove and revoke them in a timely manner. The TA must trace the malicious vehicle in the network and reveal its true identity in case of a dispute.

(x) Trust Management: A reliable trust management algorithm for vehicles is required that estimate the future trust values for vehicles by incorporating present and past trust values [31].

3) Vehicular Cloud Layer: VCC is expected to become the most economical and common platform for deploying advanced vehicular applications by reducing service provisioning time and cost. Several concerns prevent the usefulness and proper functioning of emerging vehicular clouds, and security and privacy are considered the most important issues. Many factors have potential impact on vehicular cloud security, however, it is the mobility, multitenant, and dynamic nature of the vehicular clouds that introduces additional challenging problems to the vehicular cloud environment. A VM for a single cloud member may be deployed in different physical OBUs in the vehicular cloud. However, they must be connected and secured from internal and external intrusion [83]. In addition, there may be multiple VMs on the same underlying hardware OBU and one VM can be accessed illegally by another VM on the same physical machine. As classified in [84], access control, attack detection, confidentiality, integrity, availability, security auditing, and non repudiation are used to measure the security and privacy of the cloud.

(i) Access Control: Access control is a mechanism to enforce limited and controled access to system resources, granting access only to authorized cloud entities (users, hardware devices, virtual machines, processes, programs, private information, and data).

(ii) Attack Detection: Attack detection security requirements enable the cloud system to detect, record, and notify of internal and external attacks on cloud resources.

(iii) Integrity: Integrity protection refers to the integrity of the cloud system and protects various components of the cloud system such as hardware, software, personal information and cloud data from various kinds of internal and external tampering events.

(iv) Security Auditing: This concerns the ability of security forces to audit the status and deploy security mechanisms based on the analysis of security-related events [85]. This is usually performed to ensure compliance with laws and regulations or accountability and control.

(v) Confidentiality: This security requirement enables information disclosure and data access to authorized cloud entities only. This requirement prevents sensitive information from being leaked to unauthorized entities, while ensuring that information is accessible to legitimate entities only.

(vi) Non Repudiation: This security requirement includes requirements for denying a cloud entity any form of interaction with the cloud.

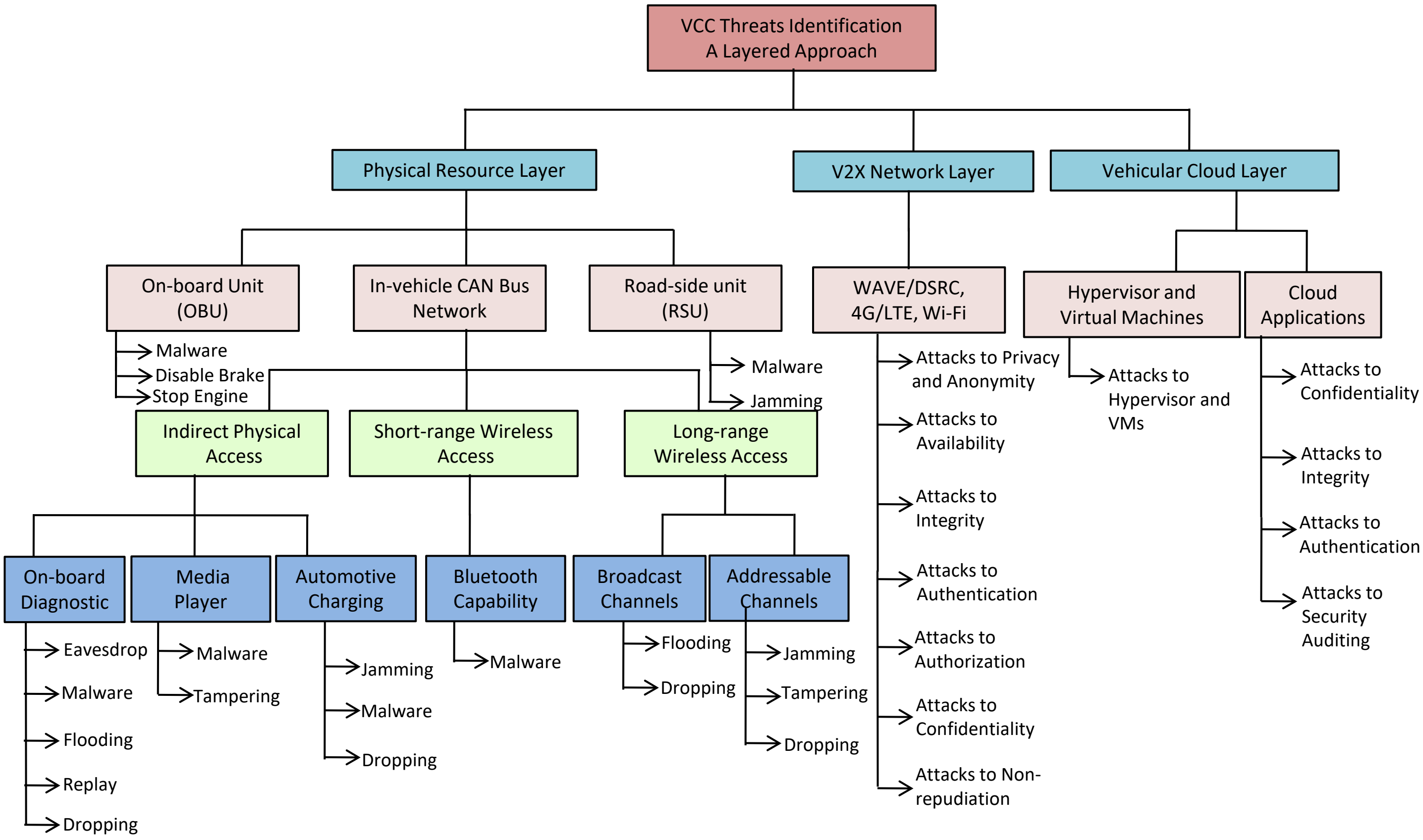

Fig. 6. Threats identification in VCC - A layered approach

B. *Threats Identification in VCC - A Layered Approach*

In this subsection, we present the proposed taxonomy of the security and privacy threats in VCC system. In a VCC system, threats can be found in various VCC components including vehicles, road-side infrastructure, wireless communications channels, messages, and shared resources between vehicles and adjacent infrastructure. Thus, we categorize the security and privacy threats based on the three resource layers VCC architectural components shown in Fig. 4. The security and privacy threats are first categorized into physical resource layer, V2X network layer, and vehicular cloud layer. The physical resource layer consists of an OBU, in-vehicle CAN bus network, and road-side unit. In a physical resource layer, security and privacy threats are further categorized based on the vulnerabilities found in the OBU, in-vehicle CAN bus network, and the RSU. The V2X network layer consists of V2V and V2I communications relying on shared wireless communication such as WAVE/DSRC, 4G/LTE, or Wi-Fi. In the V2X network layer, security and privacy threats are categorized based on the vulnerabilities found in the shared wireless communications channel. In the vehicular cloud layer, security and privacy threats are categorized based on the security loopholes and vulnerabilities found in hypervisor and virtual machines, and cloud applications. Detailed discussion of security and privacy threats and the techniques proposed to deal with those threats in the corresponding categories is presented in the subsequent sections. Fig. 6 illustrates the proposed classification of the security and privacy threats identified in VCC in the literature.

V. Physical Resource Layer Attacks and Countermeasures

This includes in-vehicle ECUs such as OBU, sensors, and RSUs. A modern vehicle is controlled and monitored by ECUs interconnected with each other via the vehicle's internal buses such as CAN or FlexRay. The CAN or FlexRay bus technology is based on broadcast communication protocols so connected ECUs are exposed to one-another, constituting an in-vehicle network attack surface. In [86], [87], the authors summarized various attack types on the in-vehicle network based on different views of varying attack modes. These attacks include eavesdropping, replay attacks, spoofing, drop, flooding, and tampering with CAN frames, and are demonstrated in Fig. 7.

Several non-trivial ECUs are also externally accessible through a wide variety of I/O interfaces that constitute an external attack surface of a car [88]. An adversary can infiltrate virtually any OBU and can leverage this ability to control a wide range of automotive functions, including disabling

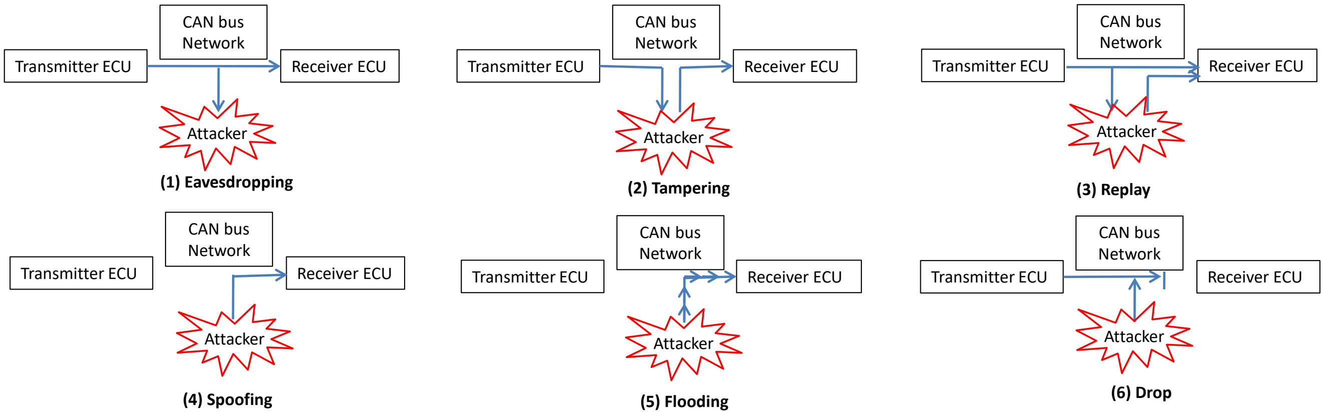

Fig. 7. Common attack scenarios to the in-vehicle network

the brakes, selectively braking individual wheels on demand, and stopping the engine. RSUs, however, are static road-side entities. An adversary may directly harm the infrastructure physically on the road or illegally access the RSU software platform to introduce malwares, thereby preventing RSUs from participating in ongoing vehicular communications and cloud participation by conducting a DoS attack [89].

According to the experiments performed by [88], in-vehicle network vulnerabilities can roughly be classified into three levels:

A. *Indirect Physical Access*

These vulnerabilities are caused by the following interfaces:

(i) On-board Diagnostics Port (OBD-II): The OBD-II port in a vehicle can access all the in-vehicle CAN buses and its connected ECUs. The OBD-II port is accessed by technicians and service personnel during routine maintenance for diagnostics such as checking the diagnostic trouble codes and upgrading an individual ECUs' firmware. In addition to its reported advantages, an OBD-II port presents significant potential for adversarial compromise. For modern vehicles, a laptop computer with installed automotive software interfaces with the pass-thru device, which in turn is connected to the car's OBD-II port. A pass-thru device is a reprogramming/diagnostic tool that connects itself with the OBD-II port and communicates with the in-vehicle network. Software running on the laptop machine can then program the vehicle's ECU using the pass-thru device. In this manner, the vehicle's ECUs are all under the control of the laptop computer. For example, an adversary can connect to the service center WiFi network and compromise a pass-thru device on the network by injecting some malicious code. The compromised pass-thru device can then compromise a far greater number of vehicles that are serviced using the malicious pass-thru device and control the data sent to the vehicle's ECUs.

(ii) Automotive Media Player: Modern vehicles with media players can interpret a wide variety of audio formats. They accept standard compact discs and plays audio by decoding the encoded audio in a variety of formats. Media player software running on the ECU handles audio parsing, and playback results are sent to the CAN bus. In this manner, an adversary can create a malicious audio file and execute the malicious code. In addition, modern vehicles include external multimedia ports such as USB iPod ports, allowing users to control multimedia inside vehicle using a smartphone or separate multimedia player. An adversary may compromise a smartphone and install software that attacks the vehicle's media system when connected.

(iii) Automotive Charging: Electric vehicles communicate with external charging infrastructure through charging cables. If an adversary can access external charging infrastructure, they can utilize that access to compromise the connected vehicle. However, these indirect physical accesses have several limitations. These limitations include complexity in operation, precise targeting, and the time of compromise.

1) Short Range Wireless Access: The short range wireless interfaces include Bluetooth, RFID keys, remote keyless entry, tire pressure monitoring system, and emerging short-range communications.

(i) Bluetooth: This has become the standard for supporting hands-free calling in vehicles. Even though the lowest level of a bluetooth protocol is implemented in the hardware, management- and services-related components are implemented through software. Modern vehicles have built-in Bluetooth capabilities (built into the vehicle's telematics unit) which allow the vehicle occupants' cell phones to connect to the vehicle and exploit vulnerabilities to execute arbitrary code on the telematics unit.

(ii) Emerging Short Range Wireless Channel: Among Wi-Fi and 3G cellular data links, an emerging wireless channel is defined in the dedicated short-range communications (DSRC) standard. Through this system, vehicles communicate digitally to inform drivers of the sudden changes in acceleration to support improved collision avoidance and harm reduction.

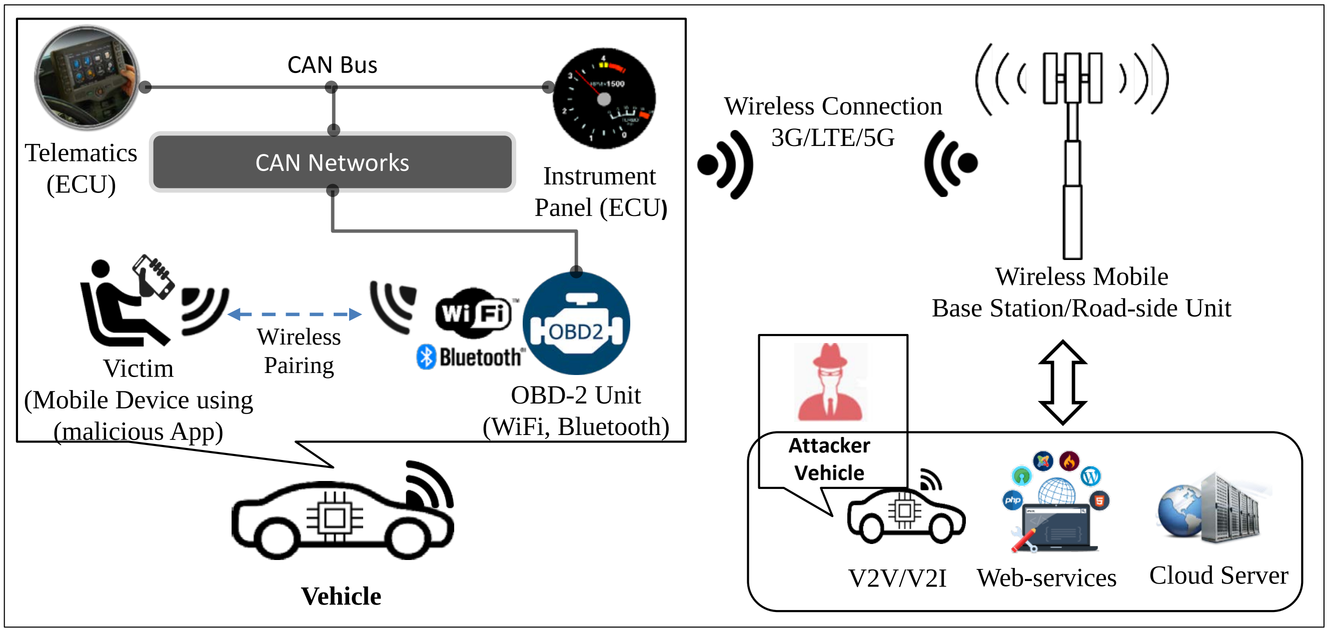

Fig. 8. A long-range wireless access in a connected car environment

B. Long Range Wireless Channels

Most manufactured vehicles include long-range (greater than 1 km) digital access channels. These long-range channels are broadly classified into two categories:

(i) Broadcast Channels: The most common and feasible way to send information to all vehicles in range at once is by simply using broadcast channels. Such broadcasts can be realized using satellite downlink, FM radio, or digital audio broadcasting (DAB) and even based on 3G/4G networks.

(ii) Addressable Channels: For wide-area connectivity, a car's telematics unit is equipped with a cell phone interface that is capable of providing voice, SMS, and 3G Internet. For the digital traffic to be relayed through this channel, the vehicle's manufacturers use the Airbiquity aqLink software modem to convert between analog and digital signals. The software creates a reliable data connection between the car's telematics unit and telematics call center. The telematics unit incorporates the aqLink code in its gateway program which controls both voice and data communications. This unit relies on the voice channel only in the case of urgent and critical situations, whereby an urgent response is required, including collision notification and accidents because this unit provides services to a wide possible area.

In [89], the authors demonstrated and evaluated attacks in two concrete forms. First, they implemented an end-to-end attack in which the running custom aqLink compatible software repeatedly calls the car for authentication until it authenticates. Secondly, the software increases the timeout from 12 to 60 seconds and then re-calls the car and exploits the buffer overflow vulnerability. Thirdly, the software forces the vehicle's telematics unit to download and execute additional payload code from the Internet using IP-addressable 3G capability. The entire attack can be implemented in a completely binding fashion without any ability to listen to the car's responses. Therefore, the in-vehicle network offers several vulnerabilities through a range of external channels. An adversary has a practical opportunity to disrupt the vehicle's internal system by gaining access to the vehicle's internal network through a range of external communication channels without having physical access to the vehicle. Using any of these capabilities (CD, Pass-thru, Bluetooth, and cellular), it is simple to command a vehicle to unlock its doors on demand. Moreover, instead of attacking a particular vehicle, the adversary might attempt to compromise as many cars as possible. During a war dialing attack, the attacker can command each car to contact a central server and report back its GPS coordinates and vehicle identification number (VIN). The attacker can search for targetted vehicles, know their positions, and then issue commands to open their doors or jam their braking system.

Automotive systems now have broad connectivity, and millions of cars on the road today can be directly addressed via cellular networks and the Internet. Security and privacy aspects of V2V and V2I communication have received significant attention from practitioners and researchers. However, the already deployed in-car sensor communication systems have gained comparatively less attention for following reasons:

- It appears that the short communication range of in-vehicular sensor networks and vehicle's metal body may make spoofing and eavesdropping attacks difficult to approach.
- Tire pressure information seems unavailable outside of

the vehicle.

Even though vehicular communications provide a broad surface for vehicular attacks, the current tire pressure systems also provide significant potential for misuse.

In [90], researchers demonstrated that tire pressure monitoring system (TPMS) communications are based on standard modulations and simple protocols. Because these protocols do not include any cryptographic mechanisms, the communication can be interpreted through reverse-engineering processes. Moreover, the implementation of the in-car system appears to fully trust all received messages without any proper message verification and validation. Therefore, spoofing and eavesdropping attacks are possible and can cause the TPMS module to malfunction. Even though a vehicle's metal body can shield wireless signals beyond the car body, the authors observed a larger than expected eavesdropping range in their experiments. TPMS messages can be correctly received within up to 10 m from the car using a usual radio antenna, and 40 m using a basic low noise amplifier. Therefore, an adversary can overhear or spoof messages from the road side or from a nearby vehicle.

Each in-vehicle sensor module includes a 32-bit immutable identifier which is a key information that assists the ECU in determining the origin of the data packet and filtering out the data packets received from other vehicles. This identifier presents the TPMs' ECU receiver with a unique sensor ID, which is sufficient information to track the vehicles. An attacker is required to possess this information and transmission protocol knowledge to extract IDs for tracking the vehicle's messages. However, the level of knowledge required by attackers differs with the nature and type of attack. For example, replay attacks must obtain frequency band information on which sensors communicate, while the spoofing of messages requires the attackers to know protocol details along with relevant knowledge of wireless radios required to transmit the messages appropriately.

Tracking involves observing identifying characteristics from a message so that multiple messages can be linked to the same vehicle. However, the success of tracking depends on whether sensor IDs are used temporarily, or over long-time intervals and the length of the sensor IDs must suffice to uniquely identify a vehicle. While tire pressure data do not require strong confidentiality, the TPMS protocols contain identifiers that can be used to track the locations of vehicles.

In [91], the authors demonstrated a practical long-range wireless attack scenario using a real vehicle and a malicious self-diagnostic smartphone application in a connected vehicle environment (see Fig. 8). The wireless attack experiment was conducted in two phases: 1) preliminary phase and 2) actual attack phase. In the preliminary phase, an automotive diagnostic tool is attached to the OBD-II port in the vehicle, and in-vehicle CAN data frames are acquired to attain control of ECUs. The in-vehicle CAN buses are monitored after connecting a laptop to an additional port in the vehicle (see Fig. 9)). Using the automotive diagnostic tool, a command is performed to forcibly actuate a certain ECU. The actual attack phase then launches an ECU forced actuation attack through the use of a malicious smartphone application. In this phase, the malicious self-diagnostic app is assumed to be installed on the driver's smartphone and is connected to the target vehicle using the vehicle's Bluetooth or Wi-Fi. The OBD-II scan tool is also installed on the vehicle and is paired with the malicious smartphone app. The malicious self-diagnostic app transmits in-vehicle CAN data frames to the attacker's server using smartphone mobile communication network. In this manner, an attacker observes the CAN status of the target vehicle and transmits a CAN data frame to force control of an arbitrary ECU. Therefore, the target vehicle is physically malfunctioned from the abnormal CAN data frames that were sent from the attacker's server. This physical attack model identifies the following vulnerabilities in an in-vehicle CAN:

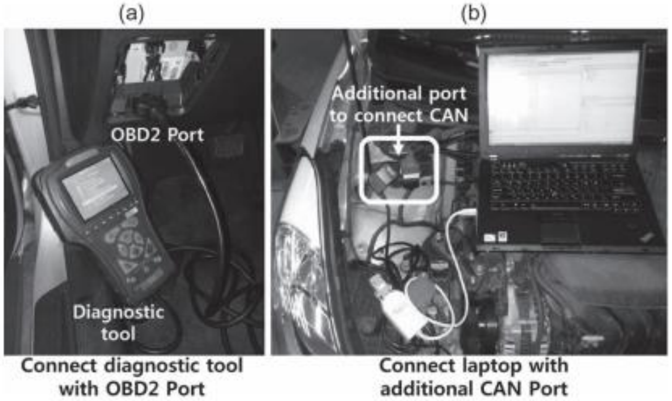
(a)
(b)
OBD2 Port
Diagnostic tool
Additional port to connect CAN
Connect diagnostic tool with OBD2 Port
Connect laptop with additional CAN Port

Fig. 9. Automotive diagnostic tool for analyzing CAN frames [91]

- Weak access control.
- No encryption.
- No authentication.

Because CAN is a broadcast communication bus system based on the sender ECUs' ID, each connected node can receive any data frame transmitted over CAN. In this manner, any compromised ECU can steal the identity of the sender node and conduct a replay attack. Because CAN is a broadcast communication protocol, ensuring access control of the broadcasted messages is impossible. Therefore, it is important to encrypt and authenticate the data frames to prevent malicious use.

The authors in [91] proposed a CAN security protocol based on an efficient data authentication technique that can also be applied to the current format of the CAN data frame. For CAN data frame encryption and authentication, a CAN security protocol must support a secure and fast key distribution mechanism. The proposed security protocol consists of long-term symmetric key and authenticated key exchange protocol 2 (AKEP2) to construct a secure and efficient key derivation process in the in-vehicle CAN. Each ECU performs encryption and authentication of the generated CAN data frames using the AES-128 and keyed-hash MAC methods respectively. When AES-128 method is applied to the 64 bit CAN data frame, the result of encryption is 128 bit. Therefore, only the first 64 bits of the AES-128 encryption are used to generate a cipher text and only 32 bit truncated MAC is used for MAC transmission. Because 32 bit MAC is not sufficient to secure a CAN data frame and an adversary can possibly leak a session key during an external device connection, encryption and authentication keys used within each session are updated periodically. Finally, additional authentication and key distribution is performed in a case, where a vehicle is connected with an external device such as, an automotive diagnostic tool.

In [92] and [80], the authors proposed communications security architecture for on-board networks using the E-safety vehicle intrusion protected applications-hardware security module (EVITA-HSM). They proposed use of symmetric cryptography in an asymmetric fashion. Moreover, they proposed the use of a truncated 32-bit MAC, considering the limited 64 bit data payload of a CAN data frame, and explained that the use of a 32-bit MAC is safe against collision attacks for 35 weeks because of certain properties of CAN such as low CAN bus speed and high CAN bus load. However, the communications architecture is quite abstract and does not provide a detailed description of the use of a 32 bit MAC. In addition, the architecture does not consider data confidentiality and the vehicle's connectivity to external devices.

[93] proposed using a pair-wise MAC which exploits the time-triggered property of ECUs and embedded systems and appends truncated MAC to each message. The proposed method also provides prevention against replay attacks by allowing the vehicles to perform pair-wise synchronization of clocks to some predefined granularity. In [94], through use cases and scenarios, the authors demonstrated the components inside a vehicle that can be protected and operations involved in ensuring the protection of the vehicle. In [95], the authors briefly surveyed the research on in-vehicle network security in a connected car environment.

In [96], the authors proposed a hybrid intrusion detection system (IDS) that can detect message injection attacks by analyzing traffic anomalies based on message frequencies. Under normal conditions, the traffic generated by each of the ECUs is cyclic and has a regular frequency or interval, e.g., message ID (0x1,0x2,...). When attackers attempt to execute a command through any ECU, the frequency or interval is unexpectedly changed for two reasons:

- Normal messages sent from ECUs.
- Injected messages sent from compromised ECUs.

Eventually, the rate of messages on the in-vehicle network is observed as a double. The authors used this traffic rate parameter as an attack detection method. The proposed system detects message injection attacks using the following procedure. When a new CAN message appears on the CAN-bus, the IDS computes the time interval from the arrival time of the latest message. If the arrival time is evaluated as being shorter than the usual interval rate, it is considered as an injected message.

Table IV shows the summary of security and privacy issues at the physical resource layer.

VI. V2X Network Layer Attacks and Countermeasures

V2X communications increase contextual awareness of vehicles on road concerning their whereabouts and warn drivers against hazardous or critical road conditions as shown in Fig. 10. Vehicles involved in V2X communications periodically broadcast status beacons (e.g., every 100 to 300 ms per vehicle [98]). These beacons provide information derived from vehicle sensors including current pseudonym, vehicle's movement information (direction, speed, acceleration or deceleration), and precise position information along with the beacon sending time. However, beacon broadcasts over wireless channel potentially threatens the security and privacy of vehicle users and their activities. An attacker can benefit from the availability of a shared wireless medium to threaten the shared medium itself and the messages relayed through it. Although the security challenges and requirements of VCC in V2X communication shares that of the conventional VANET, VCC unique features such as involvement of vehicles into multiple clouds, dynamic and temporary nature of clouds, joining of new vehicles into VC and revocation of vehicles from various clouds as well as trust issues among vehicles in VCs, make addressing the requirements a challenging task. This section focuses on security and privacy issues in V2X communications over wireless communications channel.

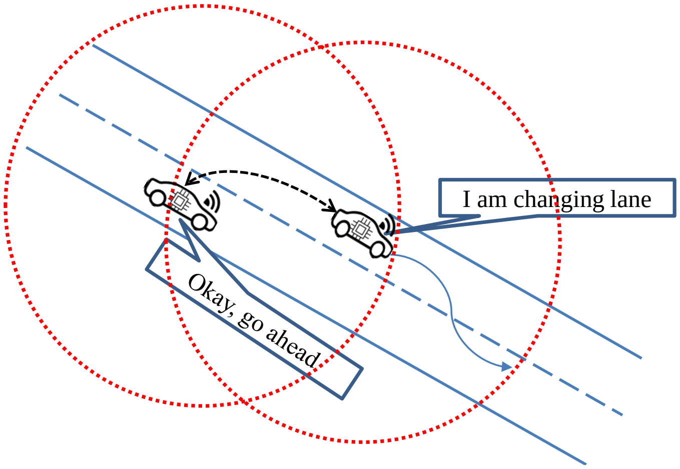

Fig. 10. V2V communication over wireless channel using DSRC

A. Attacks on Privacy and Anonymity and Countermeasures

Until recently, vehicles were not aware of the timely information of exact location and information of other vehicles. With the advent of pervasive computing applications, privacy concerns of location information have grown to a considerable scale. However, the privacy of vehicles on roads is already limited by their license plates because each vehicle is individually identifiable by its unique license plate, and therefore, it can be easily tracked [99], [100], [101]. Identity and location tracking attack is identified as the potential attack targeting the privacy of vehicular users in a V2X network. In this subsection, we provide brief description of the attacks followed by the countermeasures proposed in the literature.

In identity and location tracking attack, an attacker can deploy their eavesdropping stations, i.e., radio transceivers,

TABLE IV.
VCC SECURITY AND PRIVACY ISSUES - PHYSICAL RESOURCE LAYER

Entities Involved	Security Threats	Security Solutions	Advantages	Limitations
• ECUs • OBUs • TPMs • AU • HU • CCU • RSUs • TPMS • CANs	• Eavesdropping to the vehicular communications, • Replay of the CAN frames, • Flooding the CAN-bus to occupy network bandwidth, • Tampering with the CAN frames, • Spoofing into the in-vehicle network, • Dropping the CAN frames from reaching the destination	• Suggested a security architecture for in-vehicle network [92] [80] • Proposed a CAN security protocol consisting of long-term symmetric key and authenticated key exchange protocol (AKEP) [91] • Access control methods using data management schemes [97] • Replay protection by using secure pair-wise synchronization [93]	• They used 32-bit MAC considering limited data payload of CAN bus • Ensures data encryption and authentication, ensures secure and efficient key derivation process • Control the read and write accesses to the data and preserves the system from falsified data • Provides loss-tolerant authentication	• Security architecture is very abstract • Proposed attack model can be implemented only when driver download malicious self-diagnostic app • Digital signature od public key cryptography (PKI) based mechanism is not incorporated for further access control • This method provided bandwidth and computation overhead

ECUs - Electronic control units, OBUs - On board units, TPMs - Trusted platform modules, AU - Application unit, HU - Head unit, CCU - Communication control unit, RSUs - Road side units, TPMS - Tire pressure monitoring systems, CANs - Control area networks.

along the area it wants to remotely monitor and can automatically track vehicles and create detailed mobility patterns of vehicles. In this manner, an attacker reveals private information concerning a vehicle and its whereabouts. Such private information can be exploited for various purposes, e.g., an attacker can infer the real world identity of the user by tracing the user's home address or work place [102]. Furthermore, location tracking systems deployed by an attacker facilitate recording vehicle's movement and create enormous amounts of potentially sensitive information concerning vehicle's location privacy [103]. Therefore, anonymous vehicular communication is required to protect the privacy of individuals [104].

From a drivers' perspective, it is desirable to achieve perfect privacy. However, there exist situations in which being totally anonymous leads to several issues. For instance, location privacy needs to provide different levels of information to different users, e.g., traffic authorities, police. In [105], challenges of privacy from a driver's perspective have been discussed by proposing a privacy protocol based on access control and geolocation trust propagation mechanism. The use of access control mechanism provides privacy at different levels which was not possible with the sole use of pseudonym. However, trust evaluation based on credentials is essential to authenticate the vehicle. In [106], a concept of mix zones that ensures user privacy in location-aware services is proposed. In [107], a protocol for creating cryptographic mix-networks by using mix-zones is proposed. It connects different cryptographic mix-zones and create a large vehicular network consisting of various mix-zones. The objective of mix-networks is to achieve a large-scale location privacy by accumulating the privacy and anonymity granularity achieved by each mix-zone.

In [63], security of safety messages is addressed using anonymous public keys where anonymous keys are used to preserve privacy and contain no information about the real identity of vehicle user. In [108], a social-tier assisted packet (STAP) forwarding approach to obtain location privacy was proposed. The STAP scheme exploits characteristics of social-tiers in vehicular networks and people's lifestyle, such as well-traversed social spots to achieve location privacy [109]. In [110], a dynamic privacy-preserving key management scheme was proposed for improving the key update efficiency of location-based services (LBS) in vehicular communications. The proposed scheme not only provides fast and secure session key updates considering forward secrecy, backward secrecy, and collusion resistance but also ensures privacy-preserving authentication to vehicles. In [111], a blockchain-based architecture for protecting the privacy threats such as location tracking has been proposed. In the proposed architecture, privacy is ensured by using fresh and changeable public keys for each transaction in V2X communication. A more detailed discussion on the proposed schemes for privacy and anonymity can be found in [32], [34] listed in Section I-B.

B. Attacks on Availability and Countermeasures

Attacks on availability of the wireless network have always been the easiest type of attacks to implement, and such attacks have been highly sought out by adversaries to disrupt ongoing communications as shown in Fig. 11. The list of potential attacks targeting the availability of V2X network include jamming attack, flooding attack, blackhole attack, malware attack, spamming attack, and isolation attack. In this subsection, we provide brief description of each attack followed by the countermeasures proposed in the literature.

(i) Jamming Attack: The jamming attack is realized at the physical layer of the V2X network, and its goal is to disrupt the communication channel by transmitting noisy signals with high frequencies so as to increase the level of interference in the channel [112]. This results in a lower signal-to-noise ratio (SNR) and makes the vehicles unable to communicate with other vehicles and RSUs.

(ii) Flooding Attack: This type of attack floods the V2X network with a massive number of fake messages occupying the communications channel bandwidth with only dummy messages and thereby denying channel access to the network entities such as vehicles and RSUs [113].

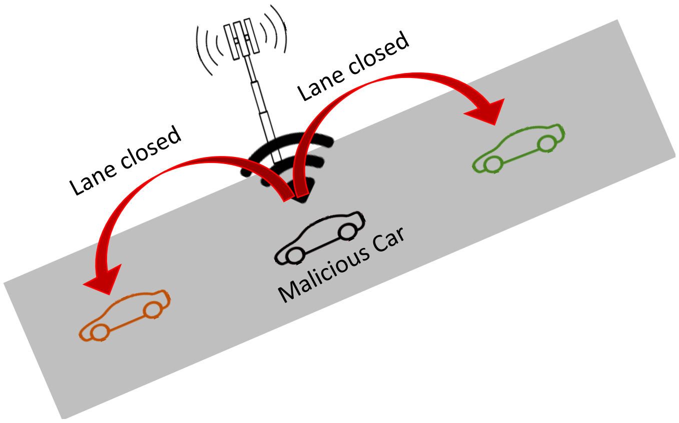

Fig. 11. Attack on availability in V2X communications

(iii) Blackhole Attack: A blackhole attack is usually caused by an internal malicious attacker [31], [61]. The attacker receives messages from the network but it does not propagate messages to other vehicles in the network and drops the messages instead as shown in Fig. 12.

(iv) Malware Attack: A malware may replicate and propagate through the network and infect V2X entities (e.g., OBU, RSU) through software components, which are used to operate OBUs and RSUs [32], [114].

(v) Spamming Attack: The spamming attack involves saturating the communications bandwidth with spam messages, i.e., advertisement messages, with the objective of unnecessarily consuming network resources and causing delay in the transmission of real messages.

(vi) Isolation Attack: In an isolation attack, an attacker maliciously isolates one or more target vehicles from participating in the network in order to affect the availability of resources in the network [32].

In the past few years, several research efforts have been undertaken to prevent attackers from attacking the availability of wireless network. The effects of jamming can be detected using techniques covered in [115] and can be mitigated by randomizing the frequency hopping spread spectrum (FHSS) mechanism of the orthogonal frequency-division multiplexing (OFDM) standard [116], which can be implemented through efficient pseudo-random generator algorithms. The high mobility of vehicles causes frequent disconnections due to which vehicles cannot access real-time information on time. In [117], an efficient data replication method for accessing vehicular applications was proposed. Data replication techniques reduce the effect of intermittent connectivity in wireless communications and improve wireless access in distributed environments. Researchers in [118], proposed an efficient data accessibility scheme by using a data replica method of RSUs to offer rapid information delivery. It allows an RSU to select the data item that must be replicated. [119] proposed an information sharing scheme to improve the accessibility of location-based data generated by vehicles on roads. A more detailed discussion on the schemes proposed for availability is provided in [32], [34] listed in Section I-B.

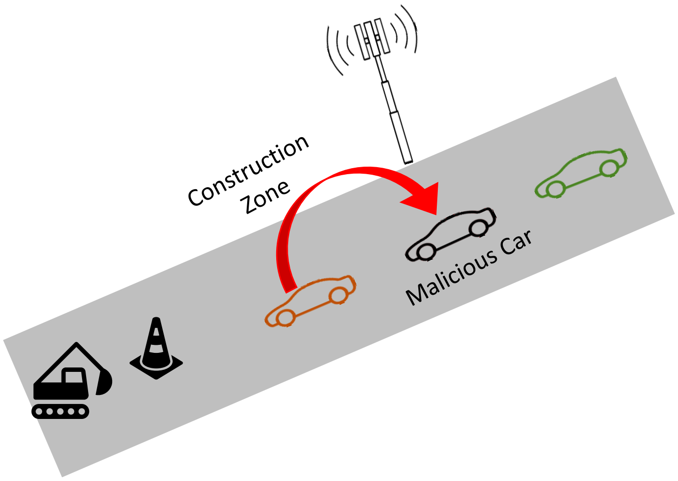

Fig. 12. Blackhole attack in V2X communications

C. Attacks on Integrity and Countermeasures

Data integrity ensures that exchanged messages are protected from unauthorized modification on the wireless communication channel. To protect data integrity, digital signatures are generated and attached with the exchanged messages [120]. The list of potential attacks targeting the integrity of V2X network include masquerading attack, data tampering attack, man-in-the-middle attack, data alteration attack, and data replay attack. In this subsection, we provide brief description of each attack followed by the countermeasures proposed in the literature.

(i) Masquerading Attack: In a masquerading attack, the attacker masquerades as the valid user's identity with an objective to produce false information and broadcast to the V2X network to achieve its targets such as slowing down the speed of vehicles. In this manner, the attacker attempts to cheat other vehicles by conveying false information.

(ii) Data Tampering Attack: This type of attack is performed by the malicious internal attacker and causes dangerous consequences to the participating vehicles in the V2X network. For example, the attacker can tamper with the integrity of the real information by fabricating fake information such as false active braking information.

(iii) Man-in-the-Middle Attack: In this attack, an attacker sits between legitimate communicating vehicles and controls communication between the two victims while legitimate vehicles believe they are directly communicating with each other as shown in Fig. 13.

(iv) Data Alteration Attack: This attack breaches the integrity of the exchanged messages by modifying, deleting, or constructing the content [67]. For instance, while outsourcing data to other vehicles, an attacker may cheat in aggregating the data it receives from its neighbor vehicles [35].

(v) Data Replay Attack: This type of attack consists of replaying (retransmitting) a previously transmitted message

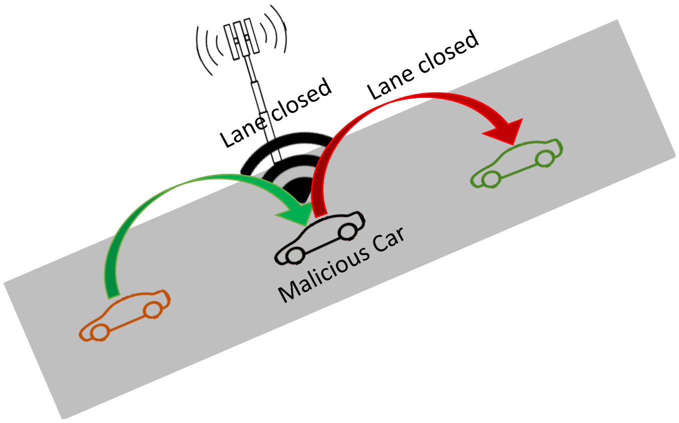

Fig. 13. Man-in-the-middle attack in V2X communications

to render false information updates to other vehicles in different V2X connections concerning the location updates or routing table updates [121].

To overcome man-in-the-middle attack, a typical cryptographic countermeasure consists of using digital certificates to authenticate legitimate vehicles is proposed in [122]. To overcome the masquerading attack, the CA issues a certificate revocation list (CRL) which maintains the identities of detected malicious vehicles, and periodically distributes the CRLs to vehicles within the network [60]. One solution to data replay attack is the implementation and maintenance of caches at the OBUs and RSUs to maintain a record of recently received messages and compare (on the basis of timestamp or sequence number) newly received messages with stored messages to reject the reception of duplicated messages. Another possible solution could be the implementation of cryptographic tokens to uniquely detect communications among V2X entities and ensure that the communication of each message is performed only once [114]. In addition to that, blockchain technique ensures correctness of data in the consensus mechanism. In this regard, [123] proposed a blockchain-based traffic event validation mechanism to achieve the reliability of confirming the event occurrences and reduce the spread of fake events from vehicles. For more details on schemes proposed for integrity, interested readers can refer [11], [24], [28], [31], [32], [34] listed in Section I-B.

D. Attacks on Authentication and Countermeasures

Authentication is the foremost security mechanism to verify the identity of vehicles and isolate legitimate vehicles from rogue and malicious ones [124] [125]. The list of potential attacks targeting on authentication include impersonation attack, sybil attack, GPS spoofing attack, tunneling attack, masquerading attack (as mentioned in Section VI-C), and man-in-the-middle attack (as mentioned in Section VI-C) [126]. In this subsection, we provide brief description of each attack followed by the countermeasures proposed in the literature.

(i) Impersonation Attack: An impersonation attack happens when an attacker successfully guesses the identities of one or more registered vehicles in V2X network, and uses those identities to inject malicious messages on behalf of other vehicles and creating chaos in a V2X network such as accidents and traffic jams [61], [127].

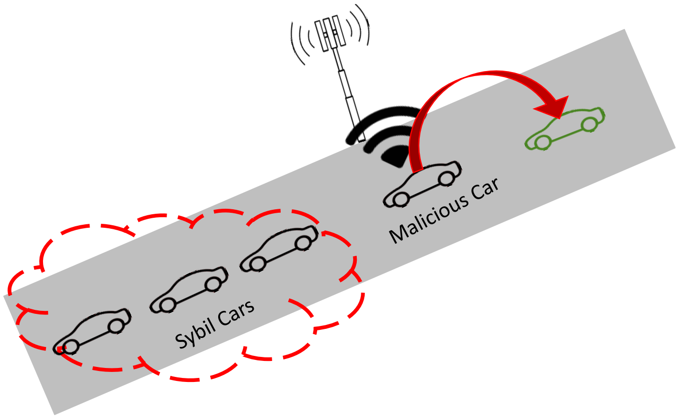

Fig. 14. Sybil Attack in V2X communications

(ii) Sybil Attack: The attacker forges multiple fake identities to simulate multiple vehicles and sends messages using multiple identities, thereby misleading the vehicles into thinking that there is a large number of vehicles in the network as shown in Fig. 14. Since a vehicle claims to be at many different locations at the same time, this makes it difficult to detect the real positions of vehicles [61], [128].

(iii) GPS Spoofing: In a GPS spoofing attack, the attacker provides false positioning information to the neighboring vehicles using a radio transmitter and GPS simulator that generates localization signals stronger than real GPS satellites. This provides false location updates to the GPS devices on the neighboring vehicles [129], [46].

(iv) Tunneling Attack: In the tunnelling attack, an attacker joins the two far-away parts in the network through an extra communication channel (tunnel), receives information at one location in the network, tunnels that into another location, and replays that information from there into the network [32], [61], [130]. For instance, an attacker can tunnel traffic information messages from a vehicle in a congested area to vehicles in a less congested area.

Several research efforts have been made to prevent attackers targeting authentication in V2X network. To overcome impersonation attack and verify the identity of vehicle in a privacy-preserving manner, [131] proposed an efficient authentication algorithm using identity-based signature (IBS). The IBS private key is generated at the cloud by using the identity of the vehicle, master key, and current time as input, and outputs vehicle's private key. Cloud generates vehicle's pseudonym, encrypts the vehicle's identifier using its private key and sends the pseudonym and private key to vehicle. When a vehicle enters in a particular region, it sends a join request to the nearby RSU using its pseudonym and IBS signature. If an attacker attempts to impersonate the identity of a vehicle, an RSU will detect the impersonation by verifying the value of current time in signature generation. After receiving the join request from vehicle, RSU forwards the request to cloud, where cloud verifies the validity of vehicle. If it is a valid vehicle, cloud sends the private key through RSU, otherwise it sends a reject message. In [132], analysis of several approaches to solving sybil attack problems has been presented. The work classifies existing approaches into different categories and discusses the advantages and limitations of each approach. [133] proposed sybil attack prevention by restricting provision of continuous timestamps to a particular vehicle within a small interval of time. At first, RSU provides a timestamp to a vehicle and sets the timer. If the vehicle requests for another timestamp with the time interval set by RSU, it is highly suspected that the vehicle is a sybil attacker and RSU denies granting timestamp.

In [134], a secure and privacy enhancing communications scheme (SPECS) has been proposed based on the idea of identity-based batch verification (IBV) [135]. In [136], vehicles obtain a digitally signed timestamp (point of time when a vehicle passes through RSU) from the RSU and attach this timestamp before sending messages. The VPKI-based solution based on a CA is considered feasible because of the deployment of a large number of vehicles from different manufacturers and countries [60]. For further details on schemes for authentication interested readers can refer [25], [30], [34] listed in section I-B.

E. Attacks on Authorization and Countermeasures

Authorization is a mechanism of enforcing access control rules to allow/deny access to the network and prevent unauthorized alteration of data on the network. Data alteration attack is identified as the potential attack targeting on authorization requirement in a V2X network. In this subsection, we provide brief description of the attack followed by the countermeasure proposed in the literature.

Data alteration attack is caused by unauthorized access to sensitive information on the network that leads to deletion, construction, or alteration of data exchanged between vehicles [151]. For instance, an attacker may alter information indicating normal congestion into a very high congestion to deceive traffic authorities. In [146], [147], a vehicular security and privacy preserving architecture was proposed focusing on authentication authorization and accountability (AAA) requirements while preserving vehicle privacy against attackers. They proposed the use of cryptographic tickets to ensure unlinkability between consecutive requests of pseudonym issuance. The author aimed to provide AAA capabilities in a VPKI according to the current vehicular communications standards.

F. Attacks on Confidentiality and Countermeasures

Vehicular communications require confidentiality of private information such as data privacy, especially in the case of Internet and RSU-based services, such as secured toll payment services, group communications, and location-based services. However, in case of exchanging safety messages, confidentiality is not required because of the high mobility of vehicles and delay involved in message encryption and decryption [152]. The list of potential attacks targeting on confidentiality of V2X network include eavesdropping attack and data interception attack. In this subsection, we provide brief description of each attack followed by the countermeasures proposed in the literature.

(i) Eavesdropping Attack: It allows an attacker to eavesdrop on the network for a certain period of time and collect sensitive information such as location information and private information of vehicles [153].
(ii) Data Interception Attack: This attack is more dangerous because it affects the privacy of vehicles since an analyzes the collected traffic information to determine the frequency of messages and types of messages being transmitted.

In [148], the authors presented a novel security scheme that provides several security services such as, privacy, confidentiality, integrity, and non-repudiation by using a crypto-based approach. The crypto-based approach uses the symmetric block cipher advanced encryption standard (AES) algorithm and a certificate-based public key infrastructure. In addition, [149] presented a blockchain-based smart contract system that provides peer-to-peer communications among V2X entities without disclosing private information using asymmetric cryptography.

G. Attacks on Non-repudiation and Countermeasures

Non-repudiation is a security service that protects vehicles against false denial of communications. Repudiation attack is identified as the potential attack targeting the non-repudiation requirement in a V2X network. In this subsection, we provide brief description of the attack followed by the countermeasure proposed in the literature.

In a repudiation attack, an attacker denies its involvement in transmitting and receiving an alleged message especially in the case of an emergency situation. The attacker's goal is to create confusion in an emergency situation for the investigation authorities to resolve the dispute. In [60], the authors proposed use of a shared session key to protect V2X communications from malicious attacks. Non-safety applications, such as traffic optimization and toll payment services, are specific to automotive domain and consider confidentiality and non-repudiation as indispensable security requirements. In [148], the authors proposed to enhance security features in [60] by extending shared session keys in non-safety applications. Furthermore, the use of blockchain in V2X communications allows vehicles to track and trace the provenance of data. Accordingly, [150] proposed to use blockchain for securing the V2X communications. The blockchain allows all transaction to be time-stamped, and encrypted with private keys. In this way, vehicles can track the history of transactions at any moment. A more detailed description on these schemes is provided in [34] listed in Section I-B. Table V shows the summary of security and privacy issues at the V2X network layer.

TABLE V.
VCC SECURITY AND PRIVACY ISSUES - V2X NETWORK LAYER

Entities Involved	Security Threats	Security Solutions	Advantages	Limitations
• Wireless access for vehicular environment (WAVE) based on IEEE 802.11 standard, • Dedicated short-range communication (DSRC), • Mobile communications network (LTE, 4G), • Public network (Wi-Fi), • Wireless sensor networks (WSNs)	• Jamming attack on the network • Flooding attack on the bandwidth • Sybil attack • Malware attack to the software • Spamming attack to the network • Eavesdropping attack on network • Data interception • Masquerading attack • Data Tampering attack • Data replay attack • Impersonation attack • GPS spoofing of the positional information • Repudiation attack • Man-in-the-middle inserts between legitimate users	• Authentication of user using vehicular public key infrastructure (VPKI) [60]	• Easy and simple authentication	• Complex management of credentials
		• Non-repudiation using shared session keys [60]	• Messages signed by sender public key	• Management of anonymous key pairs
		• Privacy-preserving authentication via RSU signature verification [134]	• Lower messages overhead	• Dependency on RSU for verification
		• Privacy using asymmetric cryptography [137], [138], [139]	• PKI-oriented security solutions	• PKI certificate issuance
		• Privacy using ID-based cryptography [140], [141], [142]	• Removes the need for public key certificates	• Introduces the problem of pseudonym issuance
		• Privacy using symmetric cryptogrpahy [143], [144]	• Computationally efficient	• Receiver is required to know secret key
		• Privacy using group signatures schemes [145]	• Reduce the need for pseudonym change	• Pseudonym resolution and revocation
		• Security of messages using anonymous public keys [63]	• Provides set of security protocols	• Key distribution is complex
		• Privacy using access control and trust using geolocation [105]	• Provides access control of the private messages	• Management of attribute parameters
		• Mix zone approach for calculating anonymity [106]	• Enhances user privacy in location services	• The solution is computationally expensive
		• Privacy based on social-tier assisted protocol [108]	• Location privacy from active global attacker	• Captures life styles to create social-tiers
		• Dynamic privacy-preserving scheme for location services [110]	• Forward and backward session key secrecy	• Deals with external attackers only
		• Blockchain-based architecture for automotive security and privacy [111]	• Increases location privacy	• Mobility and identity management
		• Frequency hopping and spread spectrum mechanism for network availability [116]	• Reduces network jamming efficiently	• Requires high capacity processors
		• Efficient data replication techniques [117]	• Improves data access through distributed	• Introduces storage overhead
		• Efficient data accessibility schemes for vehicles [118]	• Improves data accessibility through RSUs	• Introduces threat to vehicle privacy
		• Availability of data by information sharing [119]	• Improves accessibility of location data	• Suitable for static road traffic conditions
		• Blockchain based traffic event validation [123]	• Correctness of data and trust	• Cause congestion in network
		• Authentication using Identity-based signature [131]	• Efficiently calculates signatures	• Introduces threat to privacy
		• Authorization using VPKI technique [146], [147]	• Authentication, authorization, accountability	• Management of public key certificates
		• Integrity and confidentiality using crypto-based security architecture [148]	• Security based on pairwise session keys	• Requires session keys setup
		• Ethereum blockchain-based smart contract system [149]	• Allows any type of applications to run	• Power-user need to pay more than others
		• Blockchain-based trust network among vehicles [150]	• Allows track and trace provenance of data	• Difficulties with real-world usage

VII. VEHICULAR CLOUD LAYER ATTACKS AND COUNTERMEASURES

The VC layer consists of VMs created on top of physical resources, a VMM, and complex cloud applications running on the VMs. Similar to conventional cloud computing, VCC service stack also comprises the following three layers:

- Software-as-a-service.
- Platform-as-a-service.
- Infrastructure-as-a-service.

However, service providers provide services differently based on what and how the service is demanded by users. Among three layers, infrastructure-as-a-service is a fundamental service where on-board computing resources are pooled together to create advanced virtual computers and server machines with strong computing and communication capabilities. VC consumers use this service to obtain advanced VM on the move in situations that require high-processing computers to solve complicated problems such as traffic scheduling or managing evacuations. The next layer in the service stack is the platform-as-a-service layer which provides services such as http and ftp to VC users. VC users can configure these services by using APIs to develop applications that can run on the cloud such as storage functions, event handling functions, message queue functions, multi-cast functions and email functions [154]. Software-as-a-service is the top layer in the VCC service stack and provides interactive applications such as cooperative and continuous driving, driver and passenger infotainment, and vehicular Internet browsing services to VC users.

It cannot be denied that the multitenancy nature of VC introduces several security and privacy threats to VC users when sharing the same physical infrastructure with multiple VC users at the same time. A malicious user sharing the same physical resources as with others can cause several security threats to other VC users [155], [156]. VC layer primarily relies on the concept of virtualization. In the context of virtualization, the hypervisor or VMM is a system management software that allows multiple VM to be run on a single hardware at the same time while scheduling hardware resources to each guest virtual machine in a way that none of them interferes with each other.

However, compared to a non-virtualized system, the virtualization layer in VCC faces numerous security and privacy challenges. As running more VMs increases the number of VCs, vehicular resources and applications are also increased which in turn increases the number of security and privacy issues at the VC layer. Because it is difficult to keep track of all the running VMs on a distributed hardware platform of highly mobile, very interactive, and fully functional vehicles on the move, maintaining the required level of security and privacy for running VMs can be challenging. Therefore, security with respect to the hypervisor layer of VCC is a matter of great concern as all guest VMs are controlled through the hypervisor layer [157]. Compromising the hypervisor would allow an attacker to take control of the running VMs, hardware resources, and executable applications. If an attacker takes control of the hypervisor, the attacker can make malicious changes to any of the guest VMs and possess overall control of all data and processes passing through the hypervisor [158]. There may arise a situation in which a VM tries to run a malicious code on the physical resource, which brings the system down by taking full control of the system and denying access to other VMs [159]. Furthermore, once a VM is accessed illegally in a VC layer, other VMs on the same hardware resource can possibly be accessed and can attack each other because the VMs would share the same underlying hardware and software resources, including memory, device drivers, and hypervisor software. Thus, enabling virtualization to support multiple users on a shared physical infrastructure increases the VM-to-VM and VM-to-hypervisor attack potential [160].

In a virtualization environment, software applications and cloud services are virtually partitioned into multiple instances for VC users. Each VC uses its own customized instance of software applications. To interact with VC services, service providers must provide service consumers with a set of APIs. These APIs manage and control VC services. Securing a VC becomes more complex when the VC depends on these APIs to provide advanced vehicular services. Relying on insecure interfaces and poorly designed APIs allows malicious insiders to compromise the confidentiality, integrity, availability, and accountability of the service providers and VC services while accessing those services [161]. In [162], the authors addressed the problem of insecured APIs by implementing a two stage access control method at the API level that uses role based access control model (RBAC). In the first stage, a cloud user is authenticated using their credentials while their attributes are also noted. The User's role is determined by the help of their attributes. The second stage then takes over through which a user is permitted to access cloud services with the set of permissions associated with their role.

Data security and privacy protection becomes challenging at the VC layer because data are stored in a shared environment collocated with the data of other VC users. The VC user does not know where the data are stored in the VC and cannot trust and safeguard the data against intrusions. Therefore, data accesses must be secured while at rest, in transit, and in use. Standards for wireless communications protocols that use public key certificates have been developed to protect data transfers. For this purpose, cryptography key generation, key storage, and key management are usually performed outside the VC. However, mechanisms for protecting the data at rest are not well defined. Data remanence can also affect data confidentiality on the cloud. Data remanence is the residual property of data by which data remains available on the cloud even when there have been attempts to delete it. For example, if a VC user discontinues service from one VC and switches to another VC within a short period of time, a request is made to delete the discontinuing user's data stored on someone else storage. It is assumed that deleted data has been permanently deleted from the storage media immediately. However, this may not result in true removal of data. The data remains there and waits to be overwritten.

A lack of access control mechanisms may allow a malicious attacker to gain control of VMs. Therefore, as part of authentication and identity management, the ability to limit access to VCs resources is also important. Identity and access management techniques are used to provide an adequate level of protection for physical resources and data via various techniques such as login password or assigning privileges and provisioning user accounts.

A. Attacks on Hypervisor and Virtual Machines (VMs) and Countermeasures

The Hypervisor or VMM is considered as a controller that allows multiple guests VMs to be run on a single hardware at any point of time, scheduling hardware resources to each guest VM in a way that none of them interferes with each other. The list of potential attacks targeting on hypervisor and virtual machines include hyperjacking attack, bluepill attack, resource freeing attack, man-in-the-middle attack, and side channel attack. In this subsection, we provide brief description of each attack followed by the countermeasures proposed in the literature.

(i) Hyperjacking: This is an attempt to craft and run a very thin hypervisor that assumes complete control of the underlying operating system [163]. Once an attacker gains full control of the operating system, the entire cloud is compromised. The attacker will be able to eavesdrop, manipulate data, disrupt, or even shut down the entire VC service.

(ii) Bluepill Attack: The bluepill attack is a malicious code that installs itself on the fly and runs in a virtualized environment while no modifications to the system boot sector or files are required.

(iii) Resource Freeing Attack (RFA): When multiple VMs share the same physical resources on the VC, the performance of a VM will degrade if another VM is overusing physical resources. The goal of the resource freeing attack (RFA) is to modify the workload of a VM in a way that frees up physical resources for the attacker's VM, if they share a same host machine.

(iv) Man-in-the Middle Attack: [164] demonstrated a man-in-the-middle attack against a VM migration. The attacker gains administrative control of the hypervisor and VMs while a VM migrates from one physical resource to another. Hypervisor employs communication protocols to initiate a migration process and requires VM migrations to be authenticated by the migrating hosts. A man-in-the-middle attack modifies the code used for authentication and migrates a guest VM on the attacker's machine to take full control of the VM.

(v) Side Channel Attack: A side channel attack is conducted by gaining access to the physical resource hosting the target VM. This access can be made possible by creating a VM at the same physical resource that is hosting the target VM. The attacker keeps creating VMs in the VC until one VM is created at the same physical resource of the target VM. Following this, attacker can use this co-resident placement to mount cross-virtual machine side-channel attacks and extract information from the target VM on the same physical machine [165].

To overcome the hyperjacking attack, the authors in [166], suggested that new micro-processor hardware features introduced in advanced multi-core processors can protect guest VMs from malicious attacks caused by a compromised hypervisor. New hardware modifications provide facilities for protecting the confidentiality and integrity of guest VMs, while the hypervisor still manages the physical resources. Enabling the hardware modules to enforce isolation functionality more strictly and flexibly to protect guest VMs. Since hardware is logically below the hypervisor it can store data in a dedicated portion of the physical resource that cannot be altered by the hypervisor. Encryption of data and code of VMs can further defend against hypervisor attacks. [167], proposed an approach to eliminate attacks caused by the hypervisor. The proposed approach allows each VM to run natively on the underlying hardware concurrently with other VMs. Therefore, there is no need for a hypervisor to allocate system resources dynamically for VMs. This approach relies on four key ideas, 1) pre-allocating processor and memory resources needed by the VM, 2) using virtualized I/O devices, 3) minor modifications to the guest OS to enable system discovery during bootup, and 4) enabling guest VM to become in more direct contact to the underlying hardware.

B. *Attacks on Confidentiality and Countermeasures*

Confidentiality refers to the ability of authorized users to access sensitive data on the cloud [168]. Breaching confidentiality of data has always been a target for attackers in information systems. In terms of cloud computing, confidentiality is not only about securing users' confidential data. Confidentiality is also required in securing software applications hosted over VMs and VMs created over shared physical infrastructure. To prevent sensitive information from unauthorized disclosure, data on the VC must be stored in an encrypted form. However, storing cipher text might reduce the operational efficiency of the data on the VC. Because confidentiality refers to providing real data only to authentic VC users on the cloud, confidentiality can closely be coorelated with identity authentication of VC users. Identity authentication is a process of determining the confidence in a user's identity. If the authentication mechanism is weak, any attacker,can access confidential information illegally by impersonating the identity of a legitimate user.

Software confidentiality refers to the ability of software applications to be designed securely to handle sensitive data in a confidential manner. Unauthorized access to confidential data can be achieved by exploiting software vulnerabilities when a software application is designed poorly. Software applications used on the VC must be certified and protected from malicious control and have configurations to avoid security breaches. [169] proposed a confidentiality scheme that monitors access patterns for cloud services by maintaining user behavior profiling information. Whenever an unauthorized access is noticed from a malicious attacker, cloud sends decoy information to the malicious attacker as a response to the data access. The decoy information serves as a means to poison the exfilterated stolen data from cloud and confuses an attacker into thinking that they have exfilterated useful information while keeping the the real data secured. Such preventive attacks based on decoy information can provide a greater level of security on the cloud.

C. *Attacks on Integrity and Countermeasures*

Integrity refers to the ability of authorized users to modify VC assets. Authorization refers to the ability of a cloud system to determine what level of and to what extent should access to secured and private cloud resources be granted to authenticated cloud users. Strong identity and access control mechanisms ensure that cloud assets are protected from unauthorized compromise, and it can achieve unprecedented levels of confidence in VC resource integrity. Data integrity ensures that real data are protected from unauthorized deletion, modification, or fabrication. Software integrity means that software applications are protected from unauthorized modification, deletion, and fabrication. Interactive software applications use interfaces and APIs to interact with VC users. The integrity of software applications heavily depends on these interfaces and APIs. An attacker can take unauthorized control of software APIs to make changes in the software program, configurations and user's data. Hardware integrity refers to the protection of internal hardware configurations from unauthorized compromise. Issues concerning the maintenance of hardware and software integrity are expected to be controlled by the hardware owner and service provider [168].

D. *Attacks on Availability and Countermeasures*

Availability ensures that cloud resources such as data, data processing applications, and hardware resource infrastructure are accessible to authenticated and authorized users and usable when they are demanded. This includes the ability of the VC to be operational even when it suffers from a security breach [168]. In a VCC system, the nature of cloud resources

TABLE VI.
VCC SECURITY AND PRIVACY ISSUES - VEHICULAR CLOUD LAYER

Entities Involved	Security Threats	Security Solutions	Advantages	Limitations
• Vehicles as resource consumer • Vehicles as resource provider • On-board units (OBUs) • V2V communications • V2I communications • Cloud users • Virtual machine managers (VMMs) • Virtual machines (VMs) • Vehicular cloud applications	• Hyperjacking to take full control of the operating system • Traffic flow analysis by taking control of the cloud system • Bluepill by installing malicious code in operating system • Resource freeing attack by overusing the physical resources • Software modification and firmware updates • Man-in-the-middle attack during VM migration • Side channel attack • Software interruption (deletion) • Loss of data privacy • Loss of data integrity and security while at rest or in transit • Data interruption (deletion) • Impersonation attack • Denial of service (DoS)	• Role-based access control mechanism to address the problem of insecured APIs [162] • Enabling the hardware to enforce isolation functionality more strictly and store data in a dedicated portion of the hardware which cannot be altered by the hypervisor [166] • Eliminate the considerable attack surface of hypervisor by allowing VMs to run natively on the underlying hardware and allocating resources during bootup [167] • Data confidentiality by monitoring the data access patterns for cloud services by maintaining user behaviour profiling information [169] • Model based on covariance matrix mathematical method for effectively detecting flooding based DoS attacks [170] • Flooding attack prevention architecture for preventing DoS attacks [171] • Service level agreements to govern the relationship between cloud entities and explaining rights and obligations on each entity [172] • Time keeping and performance monitoring mechanisms to mitigate side-channel attacks [173]	• The mechanism is suited for the commercial needs because it helps to map a user's local role onto the role with respect to the service to be granted (global role) • This provides security for running VMs on the shared infrastructure in a way as running the applications on one's own machine • provides security by removing the possibility of interaction between guest VMs and hypervisor • Data security through preventive attacks that rely on decoy information • Effectively detects abnormal traffic • A dynamic response that can adapt to prevent any type of flooding attack • Explains the rights and responsibilities of cloud users • A comprehensive approach to mitigates all micro-architectural side channels	• This mechanism stores user's attributes and credentials during the user's registration, violating a user's privacy • it requires advanced microprocessor features which needs to be added to the new multicore processor chips • The method still requires a support for live VM migration • Introduces storage and computing overhead • Introduces computational overhead due to training phase and traffic analysis • A theoretical model only that requires performance analysis • Consumers may not carefully read the SLA and depends solely on the service provide • Requires hardware developers to design highly efficient shared micro-architectural structures

is elastic, allowing resources to be dynamically added or removed, and this requires the system to remain operational while maintaining the required level of security. Denial of service (DoS) attack is identified as the potential attack targeting on availability requirement on the VC. In this subsection, we provide brief description of the attack followed by the countermeasures proposed in the literature.

DoS attack renders the VC service inaccessible and unavailable to its authorized users when demanded. The attacker takes control and consumes a large amount of VC operational resources such as computing power, memory, and network bandwidth to disable from the authorized users. This attacks leaves cloud services to be inaccessible and affects quality of service for the authorized users. [174] classified DoS attacks broadly into two types, 1) software exploits, and 2) flooding attacks. DoS attacks based on software attempt to send fake packets with small payloads to exploit specific software vulnerabilities at the targeted software application while disabling the cloud service for an authorized user. [161] suggested schemes such as continuous patching and updating of software and firmware using firewalls and intrusion detection system for prevention from software exploit based DoS attacks. In a flooding attack, one or more attackers can execute a DoS attack by sending large amounts of fake packet requests to overwhelm the network bandwidth or operational VC resources that the VC cannot handle. [170] proposed a model based on a covariance matrix mathematical method for effectively detecting flooding based DoS attacks. The proposed model consists of three phases in which the first phase models normal traffic patterns for baseline profiling, the second phase is based on the intrusion detection processes, and the third phase prevents DoS attacks.

[171] proposed a model for preventing DoS attacks referred to as a flooding attack prevention architecture (FAPA). The FAPA model contains various components that work in collaboration to prevent the cloud from unauthorized intrusion and flooding attacks. In this approach, incoming traffic is first fed into the cloud system. Secondly, the prime information stored in the header is checked to determine if it is an abnormal traffic or regular traffic. Thirdly, the type, size, and all infrastructure details in the input traffic are verified and dynamic rules are generated by applying classifiers and link analysis to perform comparison checking for determining abnormalities in the traffic pattern. Finally, if traffic patterns are successfully verified, the request service or operation is extracted, the availability of the service is checked, and the requested service is provided to the authorized user. This approach is based on a dynamic response mechanism that can be adapted accordingly to prevent any type of flooding attacks. This model can serve as a foundation for further research on the topic of DoS flooding attack prevention.

E. Attack to Security Auditing and Countermeasure

In information security, whenever a security breach, policy violation, or other security incident occurs, a forensics investigation is necessary. Forensics investigation helps to determine the reasons behind the security breach and finds mechanisms to prevent security breaches in the future. In addition, it is always assumed that the computing media under investigation are under the complete control of the investigator. However, in a VC environment forensic investigations can be quite challenging because the evidence is likely to be ephemeral and stored on media beyond the immediate control of an investigator [172]. Thus, service level agreement (SLA), which governs the relationship between VC service consumer and service provider is required. The SLA usually explains the rights and obligations of each VC user. Many issues arise because of the SLA when the SLA is not well-defined. The consumer is unclear about what security measures are to be taken. Other issues arise because the consumer does not carefully read the SLA and depends solely on the service provider. Table VI shows the summary of security and privacy issues at the vehicular cloud layer.

VIII. Security and Privacy Issues in VCC - A System Level Perspective

VCC is a hybrid technology that exploits computing resources among vehicles, RSUs, and conventional cloud (CC) and enables interaction among vehicles, VCs, RSUs, and CC to provide advanced vehicular applications and services. Despite of the appealing advantages, security and privacy challenges are severe in VCC mainly because of the following reasons: 1) sharing of resources among untrustworthy vehicles, 2) the high mobility of vehicles causes vehicles to form different VCs with various vehicles, and 3) vehicles may need to switch and choose among several cloud service providers (CSPs). Based on the distinguished features of VCC, achieving security and privacy such as identity authentication of vehicles, key management, and vehicle location and data privacy has become challenging. For instance, high mobility of vehicles causes a vehicle to be involved in multiple VCs and authentication credentials of vehicles must be stored on each vehicle, leading to storage overhead for vehicles. Furthermore, a vehicle may access different services from multiple VCs, keeping the identity consistent during authentication to multiple VCs becomes challenging. The management of authentication credentials becomes more difficult when new vehicles join the VC. Thus, integrated authentication and key agreement (AKA) frameworks are required to provide mutual authentication and secure communications between vehicles, users, VCs, RSUs and CC. In this section, we provide discussions on the issues of security and privacy requirements, security and privacy attacks, and countermeasures at a complete system level.

A. Security and Privacy Requirements

To resist malicious attackers and provide secure communications in VCC, an AKA protocol must satisfy the following security requirements:

(i) Mutual Authentication: In order to provide reliably secure communications, vehicles, RSUs, and CC need to be authenticated by each other and should be able to verify the legitimacy of each other.

(ii) Key Agreement: After a successful authentication, vehicles, RSUs, and CC can share session keys for encrypting and decrypting the subsequent communications to achieve confidentiality and integrity of the transmitted data.

(iii) Single Sing-on: In order to access to multiple VCs securely, vehicles need to use only a single set of credentials obtained from the CC during registration.

(iv) Vehicle Anonymity: To prevent vehicles to be identified by attackers during message transmission, the authentication protocol must be able to secure real identities of vehicles.

(v) Vehicle Untraceability: The authentication protocol should be capable of providing untraceability to protect vehicle's communications in multiple VCs from being linked and traced by the attackers.

B. Security and Privacy Attacks and Countermeasures

Impersonation attack, replay attack, as well as location and identity privacy attacks are identified as major security and privacy issues, and the brief discussion of each attack as well as the countermeasures proposed in the literature are presented as follows:

(i) Impersonation Attack: An attacker can inject false information by using identity of a legitimate vehicles.

(ii) Replay Attack: During the authentication and key agreement, an attacker can replay the transmission of previously generated message in multiple VCs in order to mystify the authorities and prevent identification of vehicle.

(iii) Location and Identity Privacy: Attackers can obtain vehicle's privacy and other information in plain-text during the authentication phase.

To cope with the security and privacy challenges of AKA in VCC, in [42], an integrated AKA framework for achieving mutual authentication and secure communications between vehicles, users, VC, and CC has been proposed. The proposed framework is based on the single-server 3-factor AKA (SS-3FAKA) protocol and identity based encryption. A typical SS-3FAKA protocol involves two entities, a user and a CC, and consists of the following phases: initialization, registration, login and authentication, password and biometric change, and re-registration and revocation [175]. A CC initializes and publishes the system parameters. In order to register with CC, a user selects identifier and password, provides a biometric sample, and submits a value derived from the identifier, password, and biometric sample to cloud server through a secure communications channel. CC receives user's credentials and issues a smart card for user by storing a private key. User obtains the smart card and stores all the secret information in smart card. In the login phase, user attaches smart card with personal device, enters its identifier, password, and biometric sample. The smart card interacts with the personal device and sends an authentication request to cloud server. CC verifies the legitimacy of user and sends an authentication response message to user. However, the proposed AKA framework for VCC is based on SS-3FAKA and non-interactive identity-based cryptography in which CC generates private keys for VC and issues smart cards for vehicle users. During the VC authentication phase, VC submits its identity to the VC, which serves as its public key, and obtains a private key from the CC. During the user registration phase, a SS-3FAKA protocol is executed between user and CC. After user registration with CC, user can request a service ticket from the CC. During the authentication between user and VC, user presents its service ticket to establish a secure communications channel between user and VC. The use of non-interactive identity-based key establishment facilitates shared key between two VCs. This framework is suitable for VCC, since vehicle only needs to register with CC, and allows vehicles to join multiple dynamic and temporary VCs. Furthermore, the complexity of public key management is hidden from the user's perspective. However, the integrated AKA framework cannot be applied in the case where user and VC belong to different security domains.

With the increasing number of vehicles, cloud service providers (CSPs), and ever growing diversified demands for new vehicular services, achieving privacy-preserving authentication in multi-cloud environment is challenging because vehicle users need to switch and choose among different CSPs. To address the problem of anonymous authentication in multi-cloud environments, [55] proposed a robust and extensible authentication scheme for vehicles in a multi-cloud environment. The term multi-cloud corresponds to different services provided by multiple CSPs. The proposed authentication scheme alleviates the complexity of key management and eliminates the problem of repeated registrations of vehicles to multiple CSPs by utilizing a cloud broker (CB). The CB allows vehicles to interact through various CSPs using a single interface that connects vehicles to multiple CSPs. The CB is managed by a TA and selects appropriate CSPs for vehicles. The proposed scheme achieves anonymous authentication in the following phases. Firstly, the TA setups the whole system by initializing the private and public key parameters. After that vehicles and CSPs get registered by the TA separately. Vehicle users need to pass third login phase with the TA before they get authenticated by the CSPs. After passing the login phase successfully, vehicles want to be authenticated by the CSPs. For this purpose, vehicles send request message to the TA, instead of CSPs. The TA verifies the legitimacy of vehicles and CB managed by the TA recommends the most suitable CSPs to vehicles. Afterwards, vehicles and CSPs perform authentication with the help of TA. The proposed scheme has advantages in terms of scalability, specifically, newly added CSPs can be added in the multi-cloud service environment by registering with the TA only once. Moreover, during the authentication phase, CSPs cannot know the real identities of the vehicles, thereby ensuring vehicle privacy.

The concept of fog computing service in vehicular networks enables vehicle users to access real-time services with quality-of-service (QoS) guarantees. However, handover process for fog computing services should be handled securely in real-time, because it may lead to severe damage to fog services if attackers can spoof and expose private information exchanged between vehicles and fog nodes deployed at the RSUs. In vehicular environments, mutual authentication and session key generation is required when vehicles join a new fog node for a fog computing service. Therefore, in [176], authors proposed mutual authentication scheme for vehicles and fog nodes. Each fog node is connected to several RSUs on the road in order to allow vehicles to reliably access fog computing services using V2I communications. In order to use fog computing service from a new fog node, vehicles need to perform mutual authentication and key agreement. The proposed mutual authentication scheme is based on one-way hash function and exclusive-or operation and consists of the following steps. Users register their vehicle to CC using their personal device. CC issues credentials for the users for verifying login process and service request through a personal device. Users perform authentication with the CC by performing a login process to an already registered account through their personal device and request fog computing services after successfully being authenticated by the system. Based on the user's request, CC sends credentials to users for fog computing service. At the same time, CC sends other credentials to fog nodes for later mutual authentication with users. The proposed scheme is efficient and lightweight in securing private information due to employing the exclusive-or operation and one-way hash function.

In [177], an attribute-based signature (ABS) scheme has been utilized, in which a signer can generate a signature based on the attributes issued by the attribute authority (AA). Vehicles receive message and verify the signature by checking if the signer's attributes satisfy complex predicate policy. However, ABS brings high computation overhead. The proposed scheme outsources the heavy signing computations to the CC through RSUs. The TA initializes CC, RSUs, and vehicles. RSUs are responsible for performing access control and authenticating the origin of messages by verifying the signature of the vehicle, and if the signatures verification is passed, RSUs partially decrypt the encrypted messages and broadcasts to vehicles.

In [178], a lightweight authentication and key agreement scheme based on one-way hash function and bitwise-XOR operation has been proposed that supports three types of mutual authentication, 1) authentication and key establishment between vehicles, 2) authentication and key establishment between vehicles and their respective cluster heads, 3) authentication and key establishment between cluster heads and their respective RSUs. The proposed scheme consists of various phases including RSU registration phase, vehicle registration phase, authentication and key establishment phase, and password update phase. The TA generates and stores the credentials for each RSU in the RSU registration phase. In the vehicle registration phase, a user selects an identifier and password and sends to the TA via a secure channel. Then, it sends credentials to vehicle, which are stored in the OBU of the vehicle. In order to perform mutual authentication among two entities, the two entities authenticate each other and establish a secret session key for future communications securely. Because of the secret shared key among the two entities, it is preferred for the vehicle users to change their passwords frequently. The password change phase allows vehicle users to change their passwords anytime without any involvement of TA. Furthermore, timestamps have been used in order to prevent replay attacks.

In [179], an anonymous and lightweight authentication scheme for user and message authentication by employing smart cards has been proposed. The smart cards are used in user authentication phase, during password change phase,

TABLE VII.
VCC SECURITY AND PRIVACY ISSUES - A SYSTEM LEVEL

Reference	Security Solution	Advantages	Limitations
[55]	• An extensible and robust authentication mechanism for vehicles in a multi cloud environment by utilizing a cloud broker (CB). The proposed scheme is based on asymmetric elliptic curve cryptography (ECC).	• Alleviates the complexity of key management • Eliminates repeated registrations of vehicles to multiple CSPs. • Provides scalability and anonymous authentication.	• The proposed scheme does not provide security guarantees among V2V based cloud computing. • Vehicles are required to pass third login phase authentication with the CSPs seperately.
[42]	• An AKA framework based on single-server 3-factor AKA (SS-3FAKA) protocol and identity based encryption (IBE) achieves mutual authentication and secure communication between VC, users, vehicles, and CC.	• Integrated AKA scheme ensures essential security goals of user anonymity and untraceability, and single sign-on. • Achieves secure access to multiple VCs.	• Integrated AKA framework cannot be applied when user and VC belong to different security domain in which multiple cloud service providers co-operatively provide cloud services to users.
[176]	• A mutual authentication and session key generation scheme that is based on one-way hash function and exclusive-or operation ensures security and privacy when vehicles join a new fog node for fog computing services at the RSUs.	• The proposed scheme is efficient and light-weight in securing private information between vehicles and RSUs. • Competitive as compared with previous methods with the best performance.	• The proposed scheme does not support authentication guarantees among fog nodes and CC. • The proposed scheme does not include security features among vehicles forming a VC.
[177]	• A hierarchical attribute-based encryption (HABE) and attribute-based signature (ABS) based security framework where the sender vehicle sign message using ABS and receiver vehicle verifies signature using complex predicate policy.	• The ABS mechanism ensures anonymous authentication in VCC. • Provides secure access control using HABE framework in VCC. • Securely outsources heavy computation from OBUs to RSUs and CC.	• The ABS scheme bring high computational complexity and delay. • The proposed security solution does not include security guarantees when computations are outsourced from vehicles to other vehicles in a VC.
[178]	• A mutual authentication and key-agreement scheme that is based on one-way hash function and bit-wise XoR operation allows vehicles in a cluster authenticate with other vehicles and cluster head, while cluster head authenticates itself with the corresponding RSU also.	• Provides efficient, decentralized, and light-weight authentication between vehicles, cluster heads, and respective RSUs. • Preserves anonymity and untraceability properties as well as session key breaking attack.	• Secret session key is shared among any two entities, requiring these entities for frequent password updates. • The proposed scheme provides security guarantees only between vehicles and RSUs.
[179]	• An anonymous authentication scheme based on smart cards (ASC) protocol. The use of smart card allows dynamic generation of login identities and replaces users' real identities.	• An efficient, light-weight, and anonymous authentication scheme. • It allows an efficient password change phase without relying on TA.	• Provides performance evaluation in terms of computation overhead, packet loss ratio, and end-to-end delay, without providing detailed security analysis.
[180]	• A security solution for vehicular cloud network (VCN) environment based on the vehicular public key infrastructure (VPKI).	• Ensures privacy-preserving authentication based on the authorities seperation in the network level and between authorities using cloud services.	• Vehicles are required to perform a registration with VCSP and CLA with its new pseudonym, every time a pseudonym is expired.
[181]	• A security solution for the coexistance of EVCE computing with use of blockchain-inspired data and energy coins based on distributed consensus, in which proof of work is based on data and energy contribution amount.	• Enhances security and privacy protection with decentralization and co-participation, avoids tampering with data traceability, provides robustness against single point of failure.	• The proposed blockchain-based security framework illustrates security solution and security requirements in EVCE computing and lacks security analysis in the EVCE computing.
[182]	• A JointCloud collaboration framework of multiple VCs that uses blockchain to establish secure collaboration mechanism and focuses on VC services method and standardization method.	• Supports peer-to-peer collaboration among different VCs and automatic placement of security policies to provide resilient JointCloud security capabilities.	• The proposed technical framework describes only the high-level security policy and lacks demonstrating security analysis of the framework for JointCloud security.

and to enable secure communications after successful mutual authentication. In the user registration phase, TA assigns smart cards to vehicle users. In the user login phase, user legitimacy is checked through its smart card. Vehicle users need to be authenticated by each other and obtain session keys for future secure communications. Timestamps which are based on the GPS, are attached to the messages to validate the freshness of messages and prevent from replay attacks.

In [180], a security solution for vehicular cloud network (VCN) has been proposed. The security solution adapts public-key infrastructure (PKI) architecture in VCN environment to ensure privacy-preserving authentication. The operation of requesting pseudonym is divided into two steps. First, a vehicle sends a token request, comprising of its real identity, to the long-term certificate authority (LTCA). The LTCA replies with long-term certificate (LTC). Vehicle use this LTC to send a request to pseudonym certificate authority (PCA) for obtaining a set of pseudonyms. The PCA verifies the LTC and issues a set of pseudonyms to vehicle. Second, vehicle sends a cloud token request to cloud authority (CLA) along with the cloud account ID and pseudonym. The CLA verifies vehicle user account and sends a token for the user's account. Next, vehicle sends a cloud service request to the vehicular cloud service provider (VCSP) using its cloud token. The VCSP sends a cloud account status request message to the CLA including the token, where CLA verifies the request and sends a cloud account status reply to VCSP with the account information of vehicle user. After that, a vehicle can use cloud services using its pseudonym. However, vehicle can use cloud services for the duration of pseudonym validity. When pseudonym gets expire, vehicle needs to perform a registration with VCSP and CLA with its new pseudonym. To this end, privacy is enforced based on the authority's separation in the network level and between authorities when using cloud services.

In [181], authors proposed to use blockchain for addressing the security issues in electric vehicles cloud and edge (EVCE) computing environment. Blockchain inspired data coins have been defined as new cryptocurrency for vehicular applications and data contribution frequency is applied for proof determination. The vehicular records are encrypted and structured into the blocks based on pre-defined distributed consensus mechanism. Vehicular records are stored in the consortium blockchain during information exchange and RSUs audit the vehicular records and add them into blockchain for verification. Since it is difficult for a single cloud meet the high-quality service requirements of vehicular application, [182] proposed the collaboration framework of multiple VCs to provide reliable and secure cloud services to vehicle users. They proposed to use blockchain technology into a framework of multiple physical VCs and design a set of information and value exchange that supports independent peer-to-peer collaborations among multiple VCs. Table VII shows the summary of system level security and privacy issues in VCC.

IX. Security and Privacy Issues in VCC Applications

Different from traditional cloud computing, VCC exploits underutilized vehicular resources and dynamically allocates them to vehicles. The interactions among vehicle users, vehicular clouds, and conventional cloud provide a support for real-world applications such as data outsourcing, outsourced computation, data sharing and access control, and value-added services. However, issues concerning security and privacy are still the main obstacle in widespread adoption of VCC. In this section, we provide discussions on the research progress of security and privacy issues in various real-world applications in connected vehicular cloud computing environment, including outsourced computation, data outsourcing, data sharing and access control, as well as value-added services.

A. Security and Privacy Issues in Outsourced Computing

VCC was proposed to bring essential benefits to vehicle users, such as improving traffic safety and offering computational services to the vehicle users on road. To deal with the security and privacy issues in outsourced computing in VCC, advanced cryptographic techniques i.e., pairing-based cryptography has become an indispensable part of VCC. However, pairing computation is a time consuming operation, and the number of pairing computations could be huge in VCC because vehicles gather massive amount of road-side data from other vehicles or RSUs and require a large amount of pairing computations for data encryption and decryption. In this regard, it is necessary for vehicles to outsource the massive pairing computations to VCC while executing simple computing tasks. Current pairing computation outsourcing solutions consider all the pairing computations as a whole and outsource them to a more powerful entity, i.e., cloud for computation. However, this method is not suitable for the case in which pairing computations are outsourced from vehicle to vehicle due to the reason that various vehicles are equipped with the similar capacity of on-board resources, outsourcing all the pairing computations to one vehicle incurs a high delay on computation. Therefore, outsourcing pairing computations to a group of vehicles is considered advantageous.

In a VCC environment, three major kinds of pairing computations outsourcing services are available: outsourcing to the cloud, outsourcing to the RSU, or outsourcing to the vehicles. The cloud and RSUs are assumed to be honest-but-curious because the cloud is deployed by some high-reputation companies and RSUs are deployed by government sectors. Therefore, secure pairing computation outsourcing can be achieved when corresponding security and privacy techniques applied in conventional cloud computing are adopted in VCC. On the contrary, vehicles belong to different individuals and cannot be assumed to be trustful and honest. Vehicles may be interested in the result of outsourced pairing computations, or they may also return an arbitrary computation as a pairing computation result to save their own computations. Moreover, internal attackers can launch active attacks on the pairing computations to tamper with the integrity of computation task. Because of this different trust levels, security and privacy techniques proposed for conventional cloud computing cannot be directly applied in VCC when computation outsourcing happens between vehicles. Moreover, the existing pairing outsourcing models such as, client outsources pairing computation to one server only and client outsources pairing computations to two servers have limitations to be applied to VCC. For instance, in the former, server is assumed to be malicious, while in the later, one server is assumed to be trustful and other is assumed to be malicious. However, in a VCC environment, vehicles belong to different individuals and it is reasonable to assume every vehicle to be malicious. Hence, due to the different trust levels, these model are not suitable for VCC [52].

1) Security and Privacy Requirements: To securely and reliably outsource a series of computing tasks to a group of vehicles based on the unique features and challenges of VCC, input of the outsourcing computation needs to be protected, computation results should be verifiable, and trustworthy vehicles need to be selected to form a VC. The key security and privacy requirements for outsource computing in VCC are identified as follow [52]:

(i) Identify the Trustworthy Vehicles to Form a VC: To securely outsource sensitive computations, a vehicle is required to select trustworthy vehicles to form a VC by differentiating trust levels between vehicles, and identify the untrustworthy vehicles to block them from entering the VC.

(ii) Protect the Input and Output of the Outsourced Computation: To protect the secret information, input of the outsourced computation should be pre-processed before outsourcing the task to another vehicle for computation. For instance, in the case of pairing computation outsourcing, one input of the pairing computation during decryption is the user's private key [82]. It is also necessary to protect the result of outsourced computation because the result of outsourced computation may reveal secret information of client vehicle. For instance, the plain-text could be revealed by dividing the second part of the cipher-text to the pairing value [82].

(iii) Verifiability of the Computation Result: Because vehicles belong to different individuals, it is reasonable to suspect the outsourced computation results returned from vehicles and the validity of the returned results should be verified. Moreover, the cost of verification process should be less than that of the outsourced computation.

2) Security and Privacy Attacks and Countermeasures: In outsourced computing, data analysis and arbitrary attacks are identified as major security and privacy issues, and the brief discussion of each attack as well as the countermeasures proposed in the literature are presented as follows:

(i) Data Analysis Attack: Vehicles can analyze the outsourced computing data coming from the client vehicles. Vehicles can eavesdrop on the transmission of messages and can analyze the messages.

(ii) Arbitrary Results Attack: Vehicles have the possibility to return arbitrary computation results to the client vehicle making the final result incorrect.

To address the outsourcing computing security issues, [183] proposed a privacy-preserving trust-based verifiable VCC (PTVC) scheme. In this scheme, a trust authority generates public and private key pairs for participating vehicles and RSUs and is responsible for the maintenance and execution of the whole system. When a vehicle wants to form a VC, it finds trustworthy vehicles nearby with high reputation values using the privacy-preserving vehicle selection protocol based on a beta distribution and efficient commitment scheme [184]. Participating vehicles transfer their data securely by encrypting the outsourcing computing data, and verify the computation results with the help of privacy-preserving verifiable computing protocol based on the verification techniques used in [185], [186]. Each participating vehicle receives feedback on the performance based on which the reputation value of a vehicle is determined, which helps to identify untrustworthy vehicles and block them from participation in the VCC. Thus, the PTVC scheme not only provides anonymous authentication and trust management in VCC but also combines them with verifiable computing techniques to achieve privacy-preserving trust-based verifiable computing in VCC.

B. Security and Privacy Issues in Data Sharing and Access Control

In this subsection, we provide discussion on the research progress of security and privacy issues in data sharing and access control in VCC. With the increasing number of vehicles and popularity of advanced vehicular applications, data sharing among vehicles under emergency situations and traffic conditions is one of the most important requirements in VCC. For instance, if there is an emergency situation on the road, passing vehicles may broadcast a warning message to the nearby vehicles and may also want to notify nearby ambulance and police cars to deal with the emergency situation. Unfortunately, attackers can easily become part of VC and inject false messages into the VC communication network. Therefore, secure data sharing and fine-grained access control have become challenging issues in VCC. Current cryptography techniques, such as attribute-based encryption (ABE), are used to achieve data confidentiality and fine-grained access control for encrypted data to guarantee a controlled message access. However, applying ABE to VCC has several challenges. First, existing cryptography-based access control solutions have been proposed for the semi-trust cloud based network architectures [187], [188]. Because these cryptography-based access control schemes involve a large number of computations and vehicles' OBUs usually have limited computing resources, they may not be able to perform highly complex cryptographic operations. Secondly, attribute-based encryption brings a heavy key management burden to the attribute authority (AA). Furthermore, vehicles cannot be considered trustful or honest but curious and malicious as they belong to different individuals. Based on the above mentioned challenges, one straightforward solution is to outsource the computationally complicated encryption and decryption processes to the cloud while keeping simple and light-weight operations for the OBUs.

1) Security and Privacy Requirements: To secure data sharing in VCC and provide fine-grained access control that guarantees controlled message access, the following key security requirements are identified [54].:

(i) Data Confidentiality: Unauthorized users should not be able to access outsourced data by any means, and the outsourced encryption and decryption tasks should not leak any knowledge about data.

(ii) Vehicle Anonymity and Unlinkability: A vehicle's identity should be concealed against unauthorized users and fogs servers. Further, a vehicle's multiple accesses should not be linked by unauthorized users and fog servers.

(iii) Collude resistance: The RSUs, fogs, and cloud servers should not collude with each other for the private information in the outsourced encryption and decryption data.

2) Security and Privacy Attacks and Countermeasures: In data sharing and access control application scenario, attack on data privacy, attack on anonymity, and collusion attack are identified as major security and privacy issues, and the brief discussion of each attack as well as the countermeasures proposed in the literature are presented as follows:

(i) Attack on Data Privacy: Unauthorized users may access sensitive outsourced data and may be able to reveal plaintext from it. Moreover, fog servers are not fully trusted and may be curious about vehicle's private data.

(ii) Attack on Anonymity: Unauthorized users, fog, and cloud server can connect multiple data requests of a vehicle to reveal vehicle's identity and location privacy.

(iii) Collusion Attack: Fog servers may be able to get private information about vehicle's private data and share with each other.

To address the data sharing and access control challenges in VCC, in [54], the authors proposed a fog-to-cloud based architecture for data sharing in VCC and a cryptography-based mechanism that conducts fine-grained access control. In the proposed architecture, fog servers are deployed between cloud and network edge, only one hop from the vehicle users to provide reliable services to vehicle users. However, considering popular data sharing services, fog servers only cannot replace the cloud. Also, fog servers cannot be assumed to be fully trusted by vehicles. Thus, the proposed cryptography-based fine-grained access control scheme integrates encryption and decryption outsourcing mechanisms into the access control framework for VCC and leaves only simple tasks for vehicles. The computationally complicated task of encryption is outsourced to fog, while the computationally complicated decryption is outsourced to cloud. A vehicle generates data and uploads it in an encrypted form to the fog server. However, as a resource constrained device, it can only bear lightweight operations like symmetric cryptography. The fog server performs heavy encryption with designed access control policy. It is assumed that the fog servers obey correct access policies to encrypt the shared data. However, fog servers may be interested in the shared data before encryption. For decryption outsourcing, fog servers require storage of user's attribute keys on the fog servers which may leak user's private information. Therefore, decryption tasks are outsourced to cloud server.

In [177], a secure and efficient message access control framework has been proposed for VCC based on the hierarchical attribute-based encryption (ABE). The framework consists of a trusted authority (TA) and attribute authority (AA). The AA requests persistent attribute parameters and dynamic attribute parameters from the TA and generates persistent attribute keys and dynamic attribute keys for vehicles. The persistent attributes remain constant and consist of vehicle name or type and brand. On the other hand, dynamic attributes change frequently with time such as vehicle trajectory [189]. The cipher-text created by ABE encryption can only be decrypted if the attribute set of the receiver associated with receiver attribute keys satisfies the access policy. This technique achieves both message confidentiality and access control in VCC. To enforce message authentication, attribute-based signature (ABS) scheme has been utilized. The sender vehicle signs a message with the attributes issued by the AA. Upon receiving the message, receiver vehicle authenticates the message by checking that the sender's attributes satisfy complex predicate policy. However, ABS involves high computational complexity, which cannot be performed on resource-constrained OBUs directly. Considering the limitations of OBUs in vehicles, this scheme outsources the heavy computations from OBUs to the cloud server and RSUs.

C. Security and Privacy Issues in Data Outsourcing

VCC can save considerable time and network resources with regard to uploading content to the cloud server as a large number of vehicles can provide considerable computing, sensing, storage, and communications resources. Because vehicles are considered as ideal observation platforms for their environments and collect and store significant details in depth, VCC can provide various services to the road users, such as information dissemination and vehicular crowdsensing. Vehicular crowdsensing allows vehicles to cooperatively collect and share data about the environment, which is well beyond the capabilities of RSUs. However, the sensing data collected by vehicles may be susceptible to background noise. Thus, in order to obtain accurate sensing data, extensive research efforts have been made in vehicular crowdsensing [56], [57]. However, the challenges of security and privacy have not been addressed. In vehicular crowdsensing, fogs are utilized to process the sensing data, based on the trust discovery approaches. On one hand, fogs are not fully trusted and they are curious about vehicle's privacy. On the other hand, malicious vehicles can launch badmouth attacks by providing untruthful data. Although, attackers may be assigned low trust values, their data can still be used in calculating the truths. Moreover, some attackers can start on-off attacks in which attackers may behave honestly in the start but launch attacks when they have obtained high trust values.

1) Security and Privacy Requirements: In order to cope with the challenges of secure data outsourcing, the following security and privacy requirements must be satisfied [53]:

(i) Truth Discovery: Data generated by various vehicles may be susceptible to noise and different views of observations. It is important to obtain truthful (accurate) data from vehicles through quality-aware data aggregation and filter out the untruthful data as malicious vehicles may create inaccuracy in data.

(ii) Trust Management: A reliable trust management algorithm is required to estimate the future trust values for vehicles by incorporating present and past trust values.

(iii) Privacy Preservation: Data collected from surrounding vehicles is related to a driver's personal information including their identities, trajectories, and frequently visited places. Unauthorized users and rogue fog servers should not obtain sensitive information about vehicles and locate and spy on the vehicle's privacy.

(iv) Vehicle Authentication: To achieve privacy-preservation and conditional anonymous authentication of vehicles, an anonymous vehicle authentication mechanism is required.

2) Security and Privacy Attacks and Countermeasures: In data outsourcing application scenario, badmouth attack, identity and location privacy attack, newcomer attack, and on-off attack are identified as major security and privacy issues, and the brief discussion of each attack as well as the countermeasures proposed in the literature are presented as follows:

(i) Badmouth Attack: Malicious vehicles may launch badmouth attacks by provide untruthful data to influence the quality of data aggregation. For instance, malicious vehicles hired by a restaurant may lower reputation of some other restaurant.

(ii) Identity and Location Privacy Attack: Attackers can obtain vehicle's privacy and other information in plaintext from the vehicle's location and query contents when vehicles search for nearby restaurant or gas station.

(iii) Newcomer Attack: Malicious vehicles launching badmouth attacks may be assigned low trust values. However, malicious vehicles can register new identities to continue to launch new attacks.

(iv) On-Off Attack: It is also possible in some cases when malicious vehicles may behave normal and abnormal alternatively. For instance, malicious vehicles may behave honest to gain high trust values and start to perform badmouth attack as soon as their trust values get high enough. After that, malicious vehicles may behave honest for some time and prepare to launch attacks again.

In order to address security challenges in data outsourcing, in [53], a reliable trust-based crowdsensing scheme called RTSense has been proposed that also aims to preserve vehicle's privacy. RTSense allows vehicles to form sensing and computing VCs to collect and upload sensing data to fog servers and perform computation tasks to improve the accuracy of sensing results. RTSense removes untruthful sensing data and obtain truthful sensing results by proposing an interactive filtering truth discovery algorithm. The algorithm starts with an initial calculation of truths and achieves updates of truth values, untruthful data filtering, and truth updates iteratively, until the system gets converged. Once, truth and trust values have been obtained, TA updates the trust values of vehicles for future crowdsensing services. For this purpose, a trust management system is designed that uses aging of trust values to estimate future trust values based on the present and past trust values. In order to calculate future trust values, an exponential weighted moving average (EWMA) technique has been utilized [190]. Furthermore, to achieve privacy-preservation of vehicle's sensitive data from unauthorized users and untrustful fog, RTSense employes anonymous vehicle authentication. RTSense assumes that the VC used for computing tasks will perform computing tasks honestly. However, participating vehicles may collect and use the data determined from computing task to provide their own crowdsensing service. Hence, a grouping-based construction mechanism would provide promising solution [191]. In [192], an efficient trust-evaluation based intrusion detection mechanism for autonomous vehicular networks (AVNs) based on Q-learning has been proposed. In an AVN, autonomous driving vehicles (ADVs) send, receive, and forward messages using V2V or V2I communications and are considered as ideal candidates for environment monitoring and automated control. However, ADVs with higher automated levels are more vulnerable to inside attacks. When an ADV is compromised or hijacked by an attacker, it can generate and send false information(e.g., fake warnings) in the AVN, which will greatly affect the security of ADVs. When an ADV observes a malicious behaviour, it will generate a warning about that ADV and send to other ADVs. In order for other ADVs to trust this warning, a trust-evaluation mechanism needs to be established for ADVs. With this purpose, [192] proposed an efficient trust-evaluation mechanism, where ADVs can evaluate trust for other ADVs and send this trust value to the nearby RSUs. The RSUs exchange this trust evaluation information about ADVs through cloud. In this way, a trustworthiness of vehicle is computed by a cloud by integrating trust-evaluations of all the RSUs. The proposed trust-evaluation based intrusion detection framework comprises of two-level intrusion detections. In the first level, if an RSU receives some warning report from different ADVs, it computes a trust value of this warning based on each ADVs' trust value about the warning. In the second level, the RSU computes trust value of the warning by considering first level trust value of the warning collected from different RSUs and finding the similarities between trust value given by different RSUs. Finally, they propose to use Q-learning incentive mechanism for ADVs that stimulates ADVs to send positive reports and improve utility by maximizing trust value.

D. Security and Privacy Issues in Value-added Services

VCC improves resource utilization on vehicles and is able to support highly diverse services for vehicular users, i.e., value-added services. Such value-added services include online entertainment information, and map downloads, as well as other new vehicular services to enhance travel pleasure of vehicle users and are supported by CSPs. In this regard, vehicles would need to switch and choose among several CSPs. Considering the diverse range of value-added services and features of the VCC architecture, security and privacy challenges in VCC include mutual authentication of high mobile vehicles with CSPs, secure communications and session key management, and vehicle location and data privacy.

1) Security and Privacy Requirements: To resist malicious attackers and cope with the security challenges in value-added services, the following security and privacy requirements needs to be satisfied [55]:

(i) Mutual Authentication: In order to ensure reliability, vehicles, CSPs, and TA need to be authenticated by each

TABLE VIII.
SECURITY AND PRIVACY ISSUES IN VCC APPLICATIONS

Application Scenario	Security Threats	Security Solutions	Advantages	Limitations
Outsourced Computation	• Data analysis attack • Arbitrary result attack	• Proposed a privacy-preserving trust-based verifiable scheme in which vehicles find trustworthy nearby vehicles, and verify computing results [183]	• Provides anonymous authentication and trust management, ensures data confidentiality, and provides privacy-preserving correctness of computation results	• Does not provide support when malicious vehicles may behave honest to accumulate trust values and and start behaving malicious when their trust values are high enough.
Data Sharing and Access Control	• Privacy attack • Anonymity attack • Collusion attack	• Proposed an access control framework based on fog-to-cloud architecture with encryption and decryption outsourcing mechanism [54]. • proposed hierarchical attribute-based encryption (H-ABE) for access control and attribute-based signature (ABS) for authentication [177].	• The use of fog server helps to reduce latency and on-board device encryption burden. • Ensures message confidentiality, access control, and vehicle's authentication.	• Fog node is a semi-trust device which may not follow correct access control policy. • Due to the mobility of vehicles, maintenance of authentication credentials especially dynamic attributes becomes inefficient.
Data Outsourcing	• Badmouth attack • Privacy attack • Newcomer attack • On-off attack	• Vehicles form sensing and computing clouds to sense and improve accuracy of sensing data [53].	• Provides anonymous vehicle authentication, interactive filtering truth discovery, and reliable trust management for reliable crowdsensing	• VCs perform computing tasks. However, malicious vehicles may use sensing and computing results to provide their own crowdsensing services.
Value-added Services	• Impersonation attack • Replay attack • Privacy attack	• Proposed a robust and extensible authentication scheme for vehicles in a multi-cloud environment [55].	• Alleviates the complexity of key management and eliminates the problem of repeated registrations of vehicles to multiple CSPs by utilizing a cloud broker (CB).	• The Scheme may not perform under a VC in which neither CSP nor RSU is available.

other and should be able to verify the legitimacy of each other.

(ii) Key Agreement: After a successful authentication, vehicles and cloud service providers can share a private session key for encrypting and decrypting the subsequent communications to achieve confidentiality and integrity of the transmitted data.

(iii) Vehicle Anonymity: In order to realize the privacy protection of vehicles, the real identity of vehicle should be anonymous to all the entities.

(iv) Vehicle Untraceability: The vehicles or CSPs should not be able link the intercepted messages of the same vehicle.

(v) Traceability: The TA should be able to derive the real identity of vehicles and CSPs, when vehicles or CSPs misbehave.

2) Security and Privacy Attacks and Countermeasures: In value-added services application scenario, impersonation attack, replay attack, as well as location and identity privacy attack are identified as major security and privacy issues, and the brief discussion of each attack as well as the countermeasures proposed in the literature are presented as follows:

(i) Impersonation Attack: An attacker can inject false information by using identity of a legitimate vehicle and creating chaos such as accidents and traffic jams on behalf of other vehicles.

(ii) Replay Attack: An attacker can replay the transmission of previously generated message to mystify the authorities and prevent identification of vehicle.

(iii) Location and Identity Privacy: Attackers can obtain vehicle's privacy and other information in plain-text from the vehicle's location and service contents.

In order to cope with the challenges of increasing number of vehicles, cloud service providers (CSPs), and ever growing diversified demands for value-added services, and vehicle user's demands to switch and choose among different CSPs, [55]proposed a robust and extensible authentication scheme for vehicles in a multi-cloud environment. The proposed authentication scheme alleviates the complexity of key management and eliminates the problem of repeated registrations of vehicles to multiple CSPs by utilizing a cloud broker (CB). CB allows vehicles to interact through various CSPs using a single interface that connects vehicles to multiple CSPs. The CB is managed by a TA and selects appropriate CSPs for vehicles. The proposed scheme achieves anonymous authentication in the following phases. Firstly, the TA setups the whole system by initializing the private and public key parameters. After that vehicles and CSPs get registered by the TA separately. Vehicle users need to pass third login phase with the TA before they get authenticated by the CSPs. After passing the login phase successfully, vehicles want to be authenticated by the

CSPs. For this purpose, vehicles first send request message to the TA, instead of CSPs. The TA verifies the legitimacy of vehicles, and if the vehicle is found legal, CB managed by the TA recommends the most suitable CSPs to vehicles. Afterwards, vehicles and CSPs perform authenticate with the help of TA. The proposed scheme has advantages in terms of scalability, specifically, newly added CSPs can be added in the multi-cloud service environment by registering with the TA only once. Moreover, during the authentication phase, CSPs cannot know the real identities of the vehicles, thereby ensuring vehicle privacy. Table VIII shows the summary of security and privacy issues in VCC applications.

X. Open Issues and Future Research Directions

Currently, the concept of VCC is a technological advancement over conventional VANET service delivery model that has emerged as a promising solution to most computing problems in advanced vehicular applications. However, the deployment of VCC technology in existing VANETs is limited by several security and privacy challenges. In this section, we present open security and privacy issues and research challenges that are faced by emerging VCC technology. Providing security and privacy in VCC is relatively difficult and challenging than in conventional cloud computing and VANETs because of the special characteristics of VCC such as high mobility and short interaction of vehicles, unstable and inherently intermittent wireless connection, heterogeneous vehicular resources, dynamic resource pooling, involvement of vehicles into multiple cloud, dynamic and temporary nature of clouds, resource elasticity, maintenance of authentic credentials in various clouds, joining and revocation of vehicles into various clouds, and VM migrations. Although some of the security solutions used in cloud computing and VANET, for instance, pairing based cryptography scheme proposed for cloud computing [193] and VANET [194] to improve data access control, security of data exchanges, and achieve anonymity, can be leveraged to address the security issues in VCC [52], many security and privacy issues require new security solutions in VCC. This is due to the reason that VCC has unique features such as involvement of vehicles into multiple clouds, dynamic and temporary nature of clouds, joining of new vehicles into VC and revocation of vehicles from various clouds as well as trust issues among vehicles in VCs since different vehicles belong to different individuals in VCC, make addressing the requirements a challenging task.

A. Secure Resource Pooling:

VCC leverages underutilized computing, sensing, storage, and communication resources of vehicles to collaboratively provide advanced vehicular services and applications such as traffic management and infotainment services to end users including drivers and passengers. Despite the appealing advantages, security and privacy threats are severe due to the sharing of onboard resources among unfamiliar vehicles. The VC layer consisting of VMs created on top of onboard resources faces numerous security and privacy challenges as the number of running VMs and applications increase in VCC. Since resource sharing allows more than one VMs to be running on the same physical resource, there may be unauthorized accesses to a VM from other VMs running on the same physical resource. Thus, secured resource pooling is required in VCC.

B. Identity and Mobility Management in VCC

VCC allows mobile vehicles to share onboard resources and utilize them in areas where neither the road-side unit nor Internet cloud is available. However, the high mobility of vehicles results in rapidly changing onboard resources in the VCC. Since fast moving vehicles may form various VCs with different vehicles at different locations in order to acquire services from different VCs. Furthermore, joining of vehicles into VCs and revocation of vehicles from VCs makes the management of authentication credentials a challenging task. Thus, identity authentication of highly mobile vehicles and the management of vehicles' authentication credentials is a challenging issue in VCC. This requires for the integrated authentication and key agreement frameworks for the scalability, flexibility, and secure access to multiple VCs without requiring to register with each VC repeatedly.

C. Secure Decentralized Computing:

Different from traditional cloud computing, VCC exploits underutilized vehicular resources and dynamically allocates them to vehicles requiring more computing resources, for instance in outsourced computing application scenario, vehicles may outsource complex computing tasks to other vehicles while executing simple tasks on their onboard units. In this way, VCC operates in a decentralized way and does not require central management on early planning of resource provisioning. However, VCC confronts serious security and privacy challenges such as data security and computing security due to the attackers and legal users becoming the equipotent participants and sharing equal privileges. The sensitive data can be outsourced and processed at the attackers' onboard resource and altered without the owners' consent. Thus, it is reasonable to suspect the computing results returned by the vehicles and validity of results need to verified.

D. Secure Localization and Privacy Protection:

Several applications of VCC are based on sharing location information of vehicles and local data such as traffic management and cooperative driving. It allows potentially malicious vehicles to threaten the location privacy of vehicles and reveal the private information concerning a vehicle and its whereabouts. Such private information can be exploited for various purposes such as, an attacker can infer the real world identity of the user by tracing the user's home address or work place. In addition, sensitive data may be stored on the onboard unit of a potentially malicious vehicle at the physical resource layer. This allows malicious vehicle to make secondary usage of the stored data for its own benefits. It is also challenging to delete or bring back the private data. Therefore, anonymous vehicular communication is required to protect the location privacy of vehicles and privacy-preserving cipher-text based information storage and retrieval schemes are required to prevent disclosure of private data in VCC.

E. Secure Networking:

VCC allows vehicles to create connections based on the V2V or V2I communications. Because of the vehicles connectivity through a shared wireless medium, an attacker may threaten the shared medium itself to disrupt the VCC services and threaten the security and privacy of the messages relayed through it. An attacker can deploy its eavesdropping station along the area it wants to monitor and eavesdrop on the wireless communication channel to collect private information about vehicle. In addition, attackers can guess the identities of one or more legitimate vehicles and use those identities to inject malicious messages in the network on behave of legitimate vehicles. The attackers may also deny their involvement in injecting the alleged messages. Therefore, it is necessary to protect the messages exchanged through the shared wireless medium in VCC.

F. Heterogeneity

VCC includes vehicles with heterogeneous ECUs manufactured by various automotive companies that possess various capabilities such as speed of processor, storage capacity, and CPU power. The heterogeneous ECUs are connected via the heterogeneous bus network technologies and are exposed to one another, constituting an in-vehicle network attack surface. Although every bit of information transferred through these network media could be critical to the drivers' safety, security and privacy concerns in the design of in-vehicle communication protocols is one of the challenging issue in VCC. The connected ECUs are also externally accessible through a wide variety of I/O interface constituting an external attack surface of vehicles. It allows attackers to infiltrate virtually any onboard unit and leverage this ability to control vehicular functions. Therefore, protecting the heterogeneous in-vehicle network and physical onboard resources is a challenging issue in VCC.

G. Blockchain for VCC Security and Privacy

Blockchain includes distinguished features such as decentralization and co-participation, and is capable of addressing security issues in various networking scenarios by combining digital signatures, hash functions, cryptography, and time sequence. Although PKI-based authentication and trust-based reputation systems have been proposed in the literature to maintain privacy and anonymity, and identify the falsification of information, these methods relatively increase the amount of information exchange in VCC and result in high transmission delay. Since the blockchain has been shown to build a trust network among connected vehicles, protect the privacy, ensure the correctness of data, and achieve data access control and traceability, the applications of blockchain to VCC may confront to address the security and privacy challenges in VCC.

H. Deep Learning for VCC Security and Privacy

Existing security solutions lack sufficient functionality in capturing the dynamic behaviours of malicious vehicles in a highly dynamic VCC environment. Given that the existing security solutions may not be sufficient to meet the security and privacy challenges in VCC, it is imperative to adopt complementary measures to address the security and privacy challenges in VCC. Currently, AI and machine learning are promising techniques in developing security solutions for various dynamic network environments. For instance, due to the high mobility of vehicles in VCC, it is challenging to effectively detect the misbehavior using existing state-of-the-art techniques. Therefore, machine learning based techniques can be exploited to increase misbehaviour detection accuracy in VCC. For example, deep neural networks (DNN) can be applied in extracting features of the data shared between vehicles, training a misbehaviour classifier based on historical data that contains both the normal and attacker data, which can then be used for discriminating normal and attack behaviour. However, deep learning based approach may be limited by the misbehaviour detection latency due to the increased processing demands, and limited conditions experienced during the training of misbehaviour detection of a single vehicle. In order to overcome these challenges, VCC may exploit underutilized computing resources to form a common cloud-based infrastructure for collecting and training data regarding the normal or attack behaviour much more than in the limited conditions experienced during training of a single vehicle. In this regard, VCC can increase considerable misbehaviour detection accuracy with an increased efficiency. In addition, due to the decentralized operations in VCC, learning based distributive misbehaviour detection methods can be investigated for adaptive decision making in misbehaviour detection in VCC.

I. Edge Computing for VCC

Currently, edge computing has become a promising alternative to traditional cloud to improve VCC services by distributing computing tasks between edge resources. It may offer several advantages such as higher efficiency, lower latency, and close proximity vehicular services. Several edge computing approaches enable cloud computing capabilities at the edge of the network, including mobile edge computing (MEC), fog computing, and cloudlets. However, they possess their distinguished features. For instance, MEC servers located in close proximity to base stations (BSs) and can receive requests from vehicles and respond them directly without forwarding the request to Internet cloud. Fog computing utilizes collaborations among multiple near user edge devices or vehicles for data processing and storage. While, cloudlets can be deployed in a fully distributed manner allowing several mobile devices in close proximity to combine their computing resources locally for high demanding vehicular applications. However, despite of the potential benefits, RSUs may possess the role of integrated vehicular cloud edge computing services and cannot be fully trusted, leading to the security and privacy challenges for such integrated platforms. Therefore, security and privacy can be investigated for vehicular cloud and edge computing platforms to launch perspectives on advanced vehicular applications.

XI. Conclusion

VCC is a paradigm shift in advancements in VANETs, embedded devices, and CC technology that utilizes the rich computing resources of connected vehicles dynamically for solving unanticipated critical problems. However, in a world of black hats, technology often includes dark side as well. Therefore, considerable security and privacy challenges can be envisioned that may compromise the security and privacy of vehicles. This paper describes a layered approach to address security and privacy issues in VCC. We surveyed and analyzed security and privacy issues in the physical resource layer, V2X network layer, and vehicular cloud layer. We also addressed the security and privacy issues in VCC from a complete system perspective and with respect to the real-world applications in VCC. It is determined that some of the security solutions used in CC and VANETs may be leveraged to address the security issues in VCC. However, due to the reason that VCC has unique features such as dynamic and temporary nature of clouds, involvement of vehicles into multiple clouds, joining of vehicles into various VC, revocation of vehicles from various clouds as well as sharing resources among unfamiliar vehicles in VCC, addressing the security and privacy requirements in VCC is challenging.

References

[1] S. Abdelhamid, H. Hassanein, and G. Takahara, "Vehicle as a resource (VaaR)," *IEEE Network*, vol. 29, no. 1, pp. 12–17, 2015.

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

[3] D. Sperling and D. Gordon, "Two billion cars: transforming a culture," *TR News*, vol. 259, pp. 3–9, 2008.

[4] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," *Ad hoc networks*, pp. 1–16, 2010.

[5] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.

[6] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: a generic cloud computing model for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96–102, 2015.

[7] E. Lee, E.-K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: architecture and design principles," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 148–155, 2014.

[8] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003.

[9] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 1, pp. 284–294, 2013.

[10] M. A. Elsadig and Y. A. Fadlalla, "VANETs security issues and challenges: A survey," *Indian Journal of Science and Technology*, vol. 9, no. 28, 2016.

[11] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[12] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[13] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2017.

[14] R. Hussain and H. Oh, "Cooperation-aware VANET clouds: Providing secure cloud services to vehicular ad hoc networks." *JIPS*, vol. 10, no. 1, pp. 103–118, 2014.

[15] M. Gerla, "Vehicular cloud computing," in *Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean*. IEEE, 2012, pp. 152–155.

[16] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions," *Vehicular Communications*, vol. 9, pp. 268–280, 2017.

[17] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, 2014.

[18] L. Gu, D. Zeng, and S. Guo, "Vehicular cloud computing: A survey," in *Globecom Workshops (GC Wkshps), 2013 IEEE*. IEEE, 2013, pp. 403–407.

[19] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular cloud networks: Architecture, applications and security issues," in *Proc. of IEEE/ACM International Conference on Utility and Cloud Computing (UCC)*. IEEE, 2015, pp. 571–576.

[20] I. Ahmad, R. M. Noor, I. Ali, and M. A. Qureshi, "The role of vehicular cloud computing in road traffic management: a survey," in *International Conference on Future Intelligent Vehicular Technologies*. Springer, 2016, pp. 123–131.

[21] A. Ghazizadeh and S. Olariu, "Vehicular clouds: A survey and future directions," in *Cloud Computing for Optimization: Foundations, Applications, and Challenges*. Springer, 2018, pp. 435–463.

[22] M. R. Jabbarpour, A. Marefat, A. Jalooli, and H. Zarrabi, "Could-based vehicular networks: a taxonomy, survey, and conceptual hybrid architecture," *Wireless Networks*, vol. 25, no. 1, pp. 335–354, 2019.

[23] B. Ahmed, A. W. Malik, T. Hafeez, and N. Ahmed, "Services and simulation frameworks for vehicular cloud computing: a contemporary survey," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 4, 2019.

[24] M. Razzaque, A. Salehi, and S. M. Cheraghi, "Security and privacy in vehicular ad-hoc networks: survey and the road ahead," in *Wireless Networks and Security*. Springer, 2013, pp. 107–132.

[25] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[26] A. Luckshetty, S. Dontal, S. Tangade, and S. S. Manvi, "A survey: comparative study of applications, attacks, security and privacy in vanets," in *2016 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 2016, pp. 1594–1598.

[27] E. B. Ajulo, R. O. Akinyede, O. S. Adewale *et al.*, "Security threats and privacy issues in vehicular ad-hoc network (vanet): Survey and perspective," *Journal of Information*, vol. 4, no. 1, pp. 1–9, 2018.

[28] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2018.

[29] B. Mishra, P. Nayak, S. Behera, and D. Jena, "Security in vehicular adhoc networks: a survey," in *Proceedings of the 2011 International Conference on Communication, Computing & Security*, 2011, pp. 590–595.

[30] A. Y. Dak, S. Yahya, and M. Kassim, "A literature survey on security challenges in vanets," *International Journal of Computer Theory and Engineering*, vol. 4, no. 6, p. 1007, 2012.

[31] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Vanet security challenges and solutions: A survey," *Vehicular Communications*, vol. 7, pp. 7–20, 2017.

[32] M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services,

attacks, and applications for vehicular ad hoc networks (vanets)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.

[33] H. Khelifi, S. Luo, B. Nour, and S. C. Shah, "Security and privacy issues in vehicular named data networks: An overview," *Mobile Information Systems*, vol. 2018, 2018.

[34] M. S. Sheikh and J. Liang, "A comprehensive survey on vanet security services in traffic management system," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.

[35] L. B. Othmane, H. Weffers, M. M. Mohamad, and M. Wolf, "A survey of security and privacy in connected vehicles," in *Wireless sensor and mobile ad-hoc networks*. Springer, 2015, pp. 217–247.

[36] J. den Hartog, N. Zannone *et al.*, "Security and privacy for innovative automotive applications: A survey," *Computer Communications*, vol. 132, pp. 17–41, 2018.

[37] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging VANET with cloud computing," in *Proc. of IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2012, pp. 606–609.

[38] J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 106–113, 2014.

[39] M. R. Jabbarpour, A. Jalooli, A. Marefat, and R. M. Noor, "A taxonomy-based comparison of vehicle cloud architectures," in *Proc. of International Conference on Information and Computer Networks (ICICN 2015), Florence, Italy*, 2015.

[40] "52 percent of teens at the mall are looking for less expensive shops; 54 percent of these are shopping as much or more," https://www.prweb.com/releases/2012/9/prweb9880693.htm, September 2012, (Accessed on July 19, 2018).

[41] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds," in *Proc. of International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), 2012*. IEEE, 2012, pp. 370–375.

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

[43] J. Grover, P. Vinod, and C. Lal, *Vehicular Cloud Computing for Traffic Management and Systems*. IGI Global, 2018.

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

[45] J. Dokic, B. Müller, and G. Meyer, "European roadmap smart systems for automated driving," *European Technology Platform on Smart Systems Integration*, 2015.

[46] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent transportation systems*, vol. 16, no. 2, pp. 546–556, 2014.

[47] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1243–1274, 2018.

[48] M.-A. Lèbre, F. L. Mouël, E. Ménard, J. Dillschneider, and R. Denis, "Vanet applications: Hot use cases," *arXiv preprint arXiv:1407.4088*, 2014.

[49] L. Gu, D. Zeng, S. Guo, and B. Ye, "Leverage parking cars in a two-tier data center," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2013, pp. 4665–4670.

[50] R. Florin, S. Abolghasemi, A. G. Zadeh, and S. Olariu, "Big data in the parking lot," in *Big data management and processing*. Chapman and Hall/CRC, 2017, pp. 425–450.

[51] M. Sookhak, F. R. Yu, Y. He, H. Talebian, N. S. Safa, N. Zhao, M. K. Khan, and N. Kumar, "Fog vehicular computing: Augmentation of fog computing using vehicular cloud computing," *IEEE Vehicular Technology Magazine*, vol. 12, no. 3, pp. 55–64, 2017.

[52] J. Shao and G. Wei, "Secure outsourced computation in connected vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 36–41, 2018.

[53] L. Zhu, C. Zhang, C. Xu, and K. Sharif, "Rtsense: Providing reliable trust-based crowdsensing services in cvcc," *IEEE Network*, vol. 32, no. 3, pp. 20–26, 2018.

[54] K. Xue, J. Hong, Y. Ma, D. S. Wei, P. Hong, and N. Yu, "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 7–13, 2018.

[55] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Transactions on Information Forensics and Security*, 2019.

[56] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, and K. Ren, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems," in *Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, 2015, pp. 183–196.

[57] G. Xu, H. Li, D. Liu, H. Ren, Y. Dai, and X. Liang, "Towards efficient privacy-preserving truth discovery in crowd sensing systems," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[58] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[59] A. Panchenko and L. Pimenidis, "Towards practical attacker classification for risk analysis in anonymous communication," in *Proc. of IFIP International Conference on Communications and Multimedia Security*. Springer, 2006, pp. 240–251.

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

[61] L. Benarous, B. Kadri, and A. Bouridane, "A survey on cyber security evolution and threats: biometric authentication solutions," in *Biometric Security and Privacy*. Springer, 2017, pp. 371–411.

[62] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular cloud computing security: A survey," *Arabian Journal for Science and Engineering*, pp. 1–27, 2019.

[63] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 11–21.

[64] M. Humbert, M. H. Manshaei, J. Freudiger, and J.-P. Hubaux, "Tracking games in mobile networks," in *Proc. of International Conference on Decision and Game Theory for Security*. Springer, 2010, pp. 38–57.

[65] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *2010 Seventh international conference on wireless on-demand network systems and services (WONS)*. IEEE, 2010, pp. 176–183.

[66] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive survey on security services in vehicular ad-hoc networks," *IET Intelligent Transport Systems*, vol. 10, no. 6, pp. 379–388, 2016.

[67] A. Rawat, S. Sharma, and R. Sushil, "VANET: Security attacks and its possible solutions," *Journal of Information and Operations Management*, vol. 3, no. 1, p. 301, 2012.

[68] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[69] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, vol. 84, pp. 38–54, 2017.

[70] M. A. Khan, "A survey of security issues for cloud computing," *Journal of Network and Computer Applications*, vol. 71, pp. 11–29, 2016.

[71] S. Singh, Y.-S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[72] R. Charette, “This car runs on code,” https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, (Accessed on July,16 , 2018).

[73] T. Nolte, H. Hansson, and L. L. Bello, “Automotive communications-past, current and future.” in *ETFA*, 2005.

[74] K. H. Johansson, M. Törngren, and L. Nielsen, “Vehicle applications of controller area network,” in *Handbook of Networked and Embedded Control Systems*. Springer, 2005, pp. 741–765.

[75] W. Zeng, M. A. Khalid, and S. Chowdhury, “In-vehicle networks outlook: Achievements and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1552–1571, 2016.

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

[77] T. Hoppe, S. Kiltz, and J. Dittmann, “Security threats to automotive can networks–practical examples and selected short-term countermeasures,” in *Proc. of International Conference on Computer Safety, Reliability, and Security*. Springer, 2008, pp. 235–248.

[78] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, “Security requirements for automotive on-board networks,” in *Proc. of International Conference on Intelligent Transport Systems Telecommunications,(ITST), 2009*. IEEE, 2009, pp. 641–646.

[79] B. Schneier, “[book review] secrets and lies, digital security in a networked world,” *Economist*, vol. 356, pp. 104–104, 2000.

[80] O. Henniger, A. Ruddle, H. Seudié, B. Weyl, M. Wolf, and T. Wollinger, “Securing vehicular on-board it systems: The evita project,” in *proc. of VDI/VW Conference on Automotive Security*, 2009.

[81] E. B. Hamida, H. Noura, and W. Znaidi, “Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures,” *Electronics*, vol. 4, no. 3, pp. 380–423, 2015.

[82] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” *SIAM journal on computing*, vol. 32, no. 3, pp. 586–615, 2003.

[83] L. M. Vaquero, L. Rodero-Merino, and D. Morán, “Locking the sky: a survey on iaas cloud security,” *Computing*, vol. 91, no. 1, pp. 93–118, 2011.

[84] I. Iankoulova and M. Daneva, “Cloud computing security requirements: A systematic review,” in *Proc. of IEEE International Conference on Research Challenges in Information Science (RCIS), 2012*. IEEE, 2012, pp. 1–7.

[85] D. Firesmith, “Specifying reusable security requirements.” *Journal of Object Technology*, vol. 3, no. 1, pp. 61–75, 2004.

[86] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, and S. J. Prowell, “Modeling inter-signal arrival times for accurate detection of can bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection,” in *Proc. of the ACM Annual Conference on Cyber and Information Security Research*. ACM, 2017, p. 11.

[87] P.-S. Murvay and B. Groza, “Source identification using signal characteristics in controller area networks,” *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395–399, 2014.

[88] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, “Comprehensive experimental analyses of automotive attack surfaces.” in *Proc. of USENIX Symposium on Security*. San Francisco, 2011.

[89] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, “Experimental security analysis of a modern automobile,” in *Proc. of IEEE Symposium on Security and Privacy (SP)*, 2010, pp. 447–462.

[90] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, “Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study,” in *proc. of 19th USENIX Symposium on Security, Washington DC*, 2010, pp. 11–13.

[91] S. Woo, H. J. Jo, and D. H. Lee, “A practical wireless attack on the connected car and security protocol for in-vehicle can,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993–1006, 2015.

[92] H. Schweppe, B. Weyl, Y. Roudier, M. S. Idrees, T. Gendrullis, M. Wolf, G. Serme, S. A. De Oliveira, H. Grall, M. Sudholt *et al.*, “Securing car2x applications with effective hardware software codesign for vehicular on-board networks,” *VDI Automotive Security*, vol. 27, 2011.

[93] C. Szilagy and P. Koopman, “A flexible approach to embedded network multicast authentication,” 2008.

[94] R. Brooks, S. Sander, J. Deng, and J. Taiber, “Automobile security concerns,” *IEEE Vehicular Technology Magazine*, vol. 4, no. 2, 2009.

[95] P. Kleberger, T. Olovsson, and E. Jonsson, “Security aspects of the in-vehicle network in the connected car,” in *Proc. of IEEE Symposium on Intelligent Vehicles (IV), 2011*. IEEE, 2011, pp. 528–533.

[96] H. M. Song, H. R. Kim, and H. K. Kim, “Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network,” in *Proc. of IEEE International Conference on Information Networking (ICOIN)*. IEEE, 2016, pp. 63–68.

[97] S. Schulze, M. Pukall, G. Saake, T. Hoppe, and J. Dittmann, “On the need of data management in automotive systems.” in *BTW*, vol. 144, 2009, pp. 217–226.

[98] D. Jiang, V. Taliwal, A. Meier, W. Holfelder, and R. Herrtwich, “Design of 5.9 ghz dsrc-based vehicular safety communication,” *IEEE Wireless Communications*, vol. 13, no. 5, 2006.

[99] S. Du, M. Ibrahim, M. Shehata, and W. Badawy, “Automatic license plate recognition (alpr): A state-of-the-art review,” *IEEE Transactions on circuits and systems for video technology*, vol. 23, no. 2, pp. 311–325, 2013.

[100] A. Cavoukian, *Surveillance, then and now: Securing privacy in public spaces*. Information and Privacy Commissioner of Ontario, Canada, 2013.

[101] D. J. Glancy, “Privacy on the open road,” *Ohio NUL Rev.*, vol. 30, p. 295, 2004.

[102] J. Krumm, “Inference attacks on location tracks,” in *International Conference on Pervasive Computing*. Springer, 2007, pp. 127–143.

[103] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[104] Z. Ma, F. Kargl, and M. Weber, “A location privacy metric for V2X communication systems,” in *Proc. of IEEE Symposium on Sarnoff (SARNOFF’09)*. IEEE, 2009, pp. 1–6.

[105] J. Serna, J. Luna, and M. Medina, “Geolocation-based trust for vanet’s privacy,” in *2008 The Fourth International Conference on Information Assurance and Security*. IEEE, 2008, pp. 287–290.

[106] A. R. Beresford and F. Stajano, “Mix zones: User privacy in location-aware services,” in *proc. of IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004*. IEEE, 2004, pp. 127–131.

[107] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, “Mix-zones for location privacy in vehicular networks,” in *Proc. of ACM Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS)*, no. LCA-CONF-2007-016, 2007.

[108] X. Lin, R. Lu, X. Liang, and X. Shen, “Stap: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in vanets,” in *Prof. of IEEE INFOCOM, 2011*. IEEE, 2011, pp. 2147–2155.

[109] A. M. Vegni and V. Loscri, “A survey on vehicular social networks,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2397–2419, 2015.

[110] R. Lu, X. Lin, X. Liang, and X. Shen, “A dynamic privacy-preserving key management scheme for location-based services in VANETs,”

IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 127–139, 2012.

[111] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[112] S. O. Tengstrand, K. Fors, P. Stenumgaard, and K. Wiklundh, "Jamming and interference vulnerability of IEEE 802.11 p," in *Proc. of International Symposium on Electromagnetic Compatibility (EMC Europe), 2014*. IEEE, 2014, pp. 533–538.

[113] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)," in *Proc. of IEEE International Conference on Information Communication and Embedded Systems (ICICES), 2013*. IEEE, 2013, pp. 237–240.

[114] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (vanets): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[115] A. Hamieh, J. Ben-Othman, and L. Mokdad, "Detection of radio interference attacks in VANET," in *proc. of IEEE Conference on Global Telecommunications (GLOBECOM), 2009*. IEEE, 2009, pp. 1–5.

[116] A. M. Malla and R. K. Sahu, "Security attacks with an effective solution for dos attacks in vanet," *International Journal of Computer Applications*, vol. 66, no. 22, 2013.

[117] M. Akila and T. Iswarya, "An efficient data replication method for data access applications in vehicular ad-hoc networks," in *Proc. of IEEE International Conference on Electronics, Communication and Computing Technologies (ICECCT), 2011*. IEEE, 2011, pp. 17–22.

[118] S. Park and S. Lee, "Improving data accessibility in vehicle ad hoc network," *Int. J. Smart Home*, vol. 6, no. 4, pp. 169–176, 2012.

[119] J. Okamoto and S. Ishihara, "Distributing location-dependent data in VANETs by guiding data traffic to high vehicle density areas," in *Proc. of IEEE Vehicular Networking Conference (VNC), 2010*. IEEE, 2010, pp. 189–196.

[120] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Mobile Networking for Vehicular Environments*. IEEE, 2007, pp. 103–108.

[121] M. Mikki, Y. M. Mansour, and K. Yim, "Privacy preserving secure communication protocol for vehicular ad hoc networks," in *Proc. of IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013*. IEEE, 2013, pp. 188–195.

[122] N. Varshney, T. Roy, and N. Chaudhary, "Security protocol for vanet by using digital certification to provide security with low bandwidth," in *Proc. of IEEE International Conference on Communications and Signal Processing (ICCSP), 2014*. IEEE, 2014, pp. 768–772.

[123] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for vanets," *IEEE Access*, vol. 7, pp. 30 868–30 877, 2019.

[124] A. Daeinabi and A. G. Rahbar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," *Multimedia tools and applications*, vol. 66, no. 2, pp. 325–338, 2013.

[125] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Proc. of IEEE International Conference on Availability, Reliability and Security (ARES), 2006*. IEEE, 2006, pp. 8–pp.

[126] C. P. Pfleeger and S. L. Pfleeger, *Security in computing*. Prentice Hall Professional Technical Reference, 2002.

[127] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proc. of IEEE International Conference on Signal Processing and Communication Systems (ICSPCS), 2012*. IEEE, 2012, pp. 1–9.

[128] D. Shrivastava, A. Pandey *et al.*, "A study of sybil and temporal attacks in vehicular ad hoc networks: Types, challenges, and impacts," *International Journal of Computer Applications Technology and Research*, vol. 3, no. 5, pp. 284–291, 2014.

[129] J. S. Warner and R. G. Johnston, "Gps spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[130] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE journal on selected areas in communications*, vol. 24, no. 2, pp. 370–380, 2006.

[131] H. Goumidi, Z. Aliouat, and S. Harous, "Enhancing security communication in vehicular cloud through identifier-based-signature scheme," in *2019 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 2019, pp. 120–125.

[132] K. Kaur, S. Batish, and A. Kakaria, "Survey of various approaches to countermeasure sybil attack," *International Journal of Computer Science and Informatics*, vol. 1, no. 4, 2012.

[133] P. V. Kumar and M. Maheshwari, "Prevention of sybil attack and priority batch verification in vanets," in *Proc. of IEEE International Conference on Information Communication and Embedded Systems (ICICES)*. IEEE, 2014, pp. 1–5.

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

[135] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. of IEEE Conference on Computer Communications (INFOCOM), 2008*. IEEE, 2008, pp. 246–250.

[136] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support," in *Proc. of IEEE Military Communications Conference, MILCOM*. IEEE, 2009, pp. 1–7.

[137] L. Gollan, I. L. Gollan, and C. Meinel, "Digital signatures for automobiles?!" in *Proc. of Systemics, Cybernetics and Informatics (SCI*. Citeseer, 2002.

[138] M. El Zarki, S. Mehrotra, G. Tsudik, N. Venkatasubramanian *et al.*, "Security issues in a future vehicular network," in *European Wireless*, vol. 2, 2002.

[139] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[140] P. Kamat, A. Baliga, and W. Trappe, "An identity-based security framework for VANETs," in *Proc. of the 3rd International Workshop on Vehicular Ad Hoc Networks*. ACM, 2006, pp. 94–95.

[141] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1984, pp. 47–53.

[142] S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 380–400, 2012.

[143] J. Y. Choi, M. Jakobsson, and S. Wetzel, "Balancing auditability and privacy in vehicular networks," in *Proc. of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks*. ACM, 2005, pp. 79–87.

[144] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing privacy using symmetric random key-set in vehicular networks," in *Proc. of IEEE International Symposium on Autonomous Decentralized Systems (ISADS'07)*. IEEE, 2007, pp. 344–351.

[145] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*. ACM, 2007, pp. 19–28.

[146] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos, "Towards a secure and privacy-preserving multi-service vehicular architecture," in *Proc. of IEEE 14th International Symposium and Workshops on World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013*. IEEE, 2013, pp. 1–6.

[147] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "Vespa: Vehicular security and privacy-preserving architecture," in *Proc. of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy*. ACM, 2013, pp. 19–24.

[148] N.-W. Wang, Y.-M. Huang, and W.-M. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *Computer communications*, vol. 31, no. 12, pp. 2827–2837, 2008.

[149] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 2016, pp. 137–140.

[150] S. Kim, "Blockchain for a trust network among intelligent vehicles," in *Advances in Computers*. Elsevier, 2018, vol. 111, pp. 43–68.

[151] S. M. Safi, A. Movaghar, and M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET," in *Proc. of Second International Workshop on Computer Science and Engineering, WCSE'09*, vol. 2. IEEE, 2009, pp. 160–165.

[152] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[153] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," 2013.

[154] D. Bernstein, N. Vidovic, and S. Modi, "A cloud paas for high scale, function, and velocity mobile applications-with reference application as the fully connected car," in *2010 Fifth International Conference on Systems and Networks Communications*. IEEE, 2010, pp. 117–123.

[155] M. Pearce, S. Zeadally, and R. Hunt, "Virtualization: Issues, security threats, and solutions," *ACM Computing Surveys (CSUR)*, vol. 45, no. 2, p. 17, 2013.

[156] M. Godfrey and M. Zulkernine, "A server-side solution to cache-based side-channel attacks in the cloud," in *Proc. of IEEE International Conference on Cloud Computing (CLOUD), 2013*, 2013, pp. 163–170.

[157] S. Pal, S. Khatua, N. Chaki, and S. Sanyal, "A new trusted and collaborative agent based approach for ensuring cloud security," *arXiv preprint arXiv:1108.4100*, 2011.

[158] A. S. Ibrahim, J. Hamlyn-Harris, and J. Grundy, "Emerging security challenges of cloud virtual infrastructure," *arXiv preprint arXiv:1612.09059*, 2016.

[159] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," in *Proc. of IEEE International Conference on Cloud and Service Computing (CSC)*. IEEE, 2011, pp. 174–179.

[160] T. Ormandy, "An empirical study into the security exposure to hosts of hostile virtualized environments," 2007.

[161] M. M. Alani, "Security threats in cloud computing," in *Elements of Cloud Computing Security*. Springer, 2016, pp. 25–39.

[162] A. Sirisha and G. G. Kumari, "Api access control in cloud using the role based access control model," in *Trendz in Information Sciences & Computing (TISC), 2010*. IEEE, 2010, pp. 135–137.

[163] E. Ray and E. Schultz, "Virtualization security," in *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*. ACM, 2009, p. 42.

[164] J. Oberheide, E. Cooke, and F. Jahanian, "Empirical exploitation of live virtual machine migration," in *Proc. of BlackHat DC convention*. Citeseer, 2008.

[165] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 199–212.

[166] J. Szefer and R. B. Lee, "A case for hardware protection of guest vms from compromised hypervisors in cloud computing," in *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*. IEEE, 2011, pp. 248–252.

[167] J. Szefer, E. Keller, R. B. Lee, and J. Rexford, "Eliminating the hypervisor attack surface for a more secure cloud," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 401–412.

[168] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems*, vol. 28, no. 3, pp. 583–592, 2012.

[169] S. J. Stolfo, M. B. Salem, and A. D. Keromytis, "Fog computing: Mitigating insider data theft attacks in the cloud," in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*. IEEE, 2012, pp. 125–128.

[170] M. N. Ismail, A. Aborujilah, S. Musa, and A. Shahzad, "Detecting flooding based dos attack in cloud computing environment using covariance matrix approach," in *Proceedings of the 7th international conference on ubiquitous information management and communication*. ACM, 2013, p. 36.

[171] K. Zunnurhain, "Fapa: a model to prevent flooding attacks in clouds," in *Proceedings of the 50th Annual Southeast Regional Conference*. ACM, 2012, pp. 395–396.

[172] G. Grispos, T. Storer, and W. B. Glisson, "Calm before the storm: The challenges of cloud computing in digital forensics," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 4, no. 2, pp. 28–48, 2012.

[173] R. Martin, J. Demme, and S. Sethumadhavan, "Timewarp: rethinking timekeeping and performance monitoring mechanisms to mitigate side-channel attacks," *ACM SIGARCH Computer Architecture News*, vol. 40, no. 3, pp. 118–129, 2012.

[174] A. Hussain, J. Heidemann, and C. Papadopoulos, "A framework for classifying denial of service attacks," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2003, pp. 99–110.

[175] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826–3849, 2016.

[176] F. Dewanta and M. Mambo, "A mutual authentication scheme for secure fog computing service handover in vehicular network environment," *IEEE Access*, vol. 7, pp. 103 095–103 114, 2019.

[177] 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.

[178] M. Wazid, A. K. Das, N. Kumar, V. Odelu, A. G. Reddy, K. Park, and Y. Park, "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks," *IEEE Access*, vol. 5, pp. 14 966–14 980, 2017.

[179] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 626–10 636, 2017.

[180] D. Moussaoui, M. Feham, B. A. Bensaber, and B. Kadri, "Securing vehicular cloud networks." *International Journal of Electrical & Computer Engineering (2088-8708)*, vol. 9, 2019.

[181] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Network*, vol. 32, no. 3, pp. 78–83, 2018.

[182] B. Yin, L. Mei, Z. Jiang, and K. Wang, "Joint cloud collaboration mechanism between vehicle clouds based on blockchain," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE, 2019, pp. 227–2275.

[183] C. Huang, R. Lu, H. Zhu, H. Hu, and X. Lin, "Ptvc: achieving privacy-preserving trust-based verifiable vehicular cloud computing," in *2016 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2016, pp. 1–6.

[184] G. Arfaoui, J.-F. Lalande, J. Traoré, N. Desmoulins, P. Berthomé, and S. Gharout, "A practical set-membership proof for privacy-preserving nfc mobile ticketing," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 25–45, 2015.

[185] L. F. Zhang and R. Safavi-Naini, "Batch verifiable computation of

outsourced functions," *Designs, Codes and Cryptography*, vol. 77, no. 2-3, pp. 563–585, 2015.

[186] L. F. Zhang, R. Safavi-Naini, and X. W. Liu, "Verifiable local computation on distributed data," in *Proceedings of the 2nd international workshop on Security in cloud computing*, 2014, pp. 3–10.

[187] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 676–688, 2016.

[188] K. Xue, Y. Xue, J. Hong, W. Li, H. Yue, D. S. Wei, and P. Hong, "Raac: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 953–967, 2017.

[189] Y. Xia, W. Chen, X. Liu, L. Zhang, X. Li, and Y. Xiang, "Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2629–2641, 2017.

[190] A. C. K. Vendramin, A. Munaretto, M. R. Delgado, and A. C. Viana, "Grant: Inferring best forwarders from complex networks' dynamics through a greedy ant colony optimization," *Computer Networks*, vol. 56, no. 3, pp. 997–1015, 2012.

[191] C. Liu, L. Zhu, M. Wang, and Y.-A. Tan, "Search pattern leakage in searchable encryption: Attacks and new construction," *Information Sciences*, vol. 265, pp. 176–188, 2014.

[192] R. Xing, Z. Su, N. Zhang, Y. Peng, H. Pu, and J. Luo, "Trust-evaluation-based intrusion detection and reinforcement learning in autonomous driving," *IEEE Network*, vol. 33, no. 5, pp. 54–60, 2019.

[193] M. Morales-Sandoval, J. L. Gonzalez-Compean, A. Diaz-Perez, and V. J. Sosa-Sosa, "A pairing-based cryptographic approach for data security in the cloud," *International Journal of Information Security*, vol. 17, no. 4, pp. 441–461, 2018.

[194] C.-L. Chen, J. Shin, Y.-T. Tsai, A. Castiglione, and F. Palmieri, "Securing information exchange in vanets by using pairing-based cryptography," *International Journal of Foundations of Computer Science*, vol. 28, no. 06, pp. 781–797, 2017.

Arooj Masood received the B.S degree in computer science from Lahore College for Women University, Lahore, Pakistan, in 2011, and M.S degree in computer science from Lahore College for Women University, Lahore, Pakistan, in 2013. She is currently pursuing the Ph. D. degree at the Chung-Ang University, Seoul, South Korea. She was a Lecturer with the Department of Computer Science, Government College for Women Gulberg, Lahore, Pakistan. Her current research interests include vehicular cloud computing, ubiquitous computing, wireless networks, deep space networks, and deep reinforcement learning.

Demeke Shumeye Lakew received the B.S. degree in computer science from Hawassa University, Hawassa, Ethiopia, and the M.S. degree in computer science from Addis Ababa University, Addis Ababa, Ethiopia, in 2006 and 2011 respectively. He is currently pursuing the Ph.D. degree in computer science and engineering with the School of Computer Science and Engineering, Chung-Ang University, Seoul, South Korea. He was a Lecturer with the College of Informatics, Kombolcha Institute of Technology, Wollo University, Dessie, Ethiopia. His current research interests include flying ad hoc network, vehicular social network, traffic engineering, and reinforcement learning.

Sungrae Cho is a professor with the school of computer sciences and engineering, Chung-Ang University (CAU), Seoul. Prior to joining CAU, he was an assistant professor with the department of computer sciences, Georgia Southern University, Statesboro, GA, USA, from 2003 to 2006, and a senior member of technical staff with the Samsung Advanced Institute of Technology (SAIT), Kiheung, South Korea, in 2003. From 1994 to 1996, he was a research staff member with electronics and telecommunications research institute (ETRI), Daejeon, South Korea. From 2012 to 2013, he held a visiting professorship with the national institute of standards and technology (NIST), Gaithersburg, MD, USA. He received the B.S. and M.S. degrees in electronics engineering from Korea University, Seoul, South Korea, in 1992 and 1994, respectively, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2002.

His current research interests include wireless networking, ubiquitous computing, and ICT convergence. He has been a subject editor of IET Electronics Letter since 2018, and was an area editor of Ad Hoc Networks Journal (Elsevier) from 2012 to 2017. He has served numerous international conferences as an organizing committee chair, such as IEEE SECON, ICOIN, ICTC, ICUFN, TridentCom, and the IEEE MASS, and as a program committee member, such as IEEE ICC, GLOBECOM, VTC, MobiApps, SENSORNETS, and WINSYS.