IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 7, 2022, accepted May 8, 2022, date of publication May 12, 2022, date of current version May 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3174554

Securing Real-Time Video Surveillance Data in Vehicular Cloud Computing: A Survey

MAJED S. ALSAYFI[1,2], MOHAMED Y. DAHAB[2], FATHY E. EASSA[2], REDA SALAMA[3], SEIF HARIDI[4], AND ABDULLAH S. AL-GHAMDI[5]

[1]Department of Computer Science, College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[2]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3]Department of Information Technology, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[4]KTH Royal Institute of Technology, 114 28 Stockholm, Sweden
[5]Department of Information System, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Corresponding author: Majed S. Alsayfi (msalamahalsayfi@stu.kau.edu.sa)

This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia, under Grant KEP-PHD-21-611-42.

ABSTRACT Vehicular ad hoc networks (VANETs) have received a great amount of interest, especially in wireless communications technology. In VANETs, vehicles are equipped with various intelligent sensors that can collect real-time data from inside and from surrounding vehicles. These real-time data require powerful computation, processing, and storage. However, VANETs cannot manage these real-time data because of the limited storage capacity in on board unit (OBU). To address this limitation, a new concept is proposed in which a VANET is integrated with cloud computing to form vehicular cloud computing (VCC) technology. VCC can manage real-time services, such as real-time video surveillance data that are used for monitoring critical events on the road. These real-time video surveillance data include highly sensitive data that should be protected against intruders in the networks because any manipulation, alteration, or sniffing of data will affect a driver's life by causing improper decision-making. The security and privacy of real-time video surveillance data are major challenges in VCC. Therefore, this study reviewed the importance of the security and privacy of real-time video data in VCC. First, we provide an overview of VANETs and their limitations. Second, we provide a state-of-the-art taxonomy for real-time video data in VCC. Then, the importance of real-time video surveillance data in both fifth generation (5G), and sixth generation (6G) networks is presented. Finally, the challenges and open issues of real-time video data in VCC are discussed.

INDEX TERMS 5G, 6G, privacy, security, vehicular ad hoc network, vehicular cloud computing, real-time video data.

I. INTRODUCTION

Intelligent transportation systems (ITSs) play an important role in making the life of passengers and drivers easier and safer. ITSs aim to improve traffic efficiency by reducing traffic problems (such as traffic jams and accidents) and controlling any critical events that happen on the road. Moreover, ITSs not only focus on providing traffic safety for drivers and pedestrians on the road but also providing entertainment services to the vehicles during travel. Due to the many traffic accidents in the world today, vehicle factories have sought to develop intelligent vehicle systems to provide safety for drivers and passengers. In a recent study, the number of deaths worldwide due to traffic accidents reached one million and twenty-four thousand, which is a very large number. In addition, a million drivers are injured in the United States of America alone [1]. This high number of accidents has led to the production of modern vehicles with a high level of safety (as compared to the safety of traditional vehicles) to help reduce the number of traffic accidents.

Moreover, modern vehicles are equipped with various sensors, such as those for oil, breaks, blind spots, global positioning systems (GPS), LiDAR, and cameras. These sensors can collect safety and non-safety information regarding road status and can share or exchange data with other vehicles. In the near future, mobile communication is expected to be an integral part of vehicles. A VANET is a subtype of mobile ad hoc network (MANET) [2]–[6]. VANETs [7] aim

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

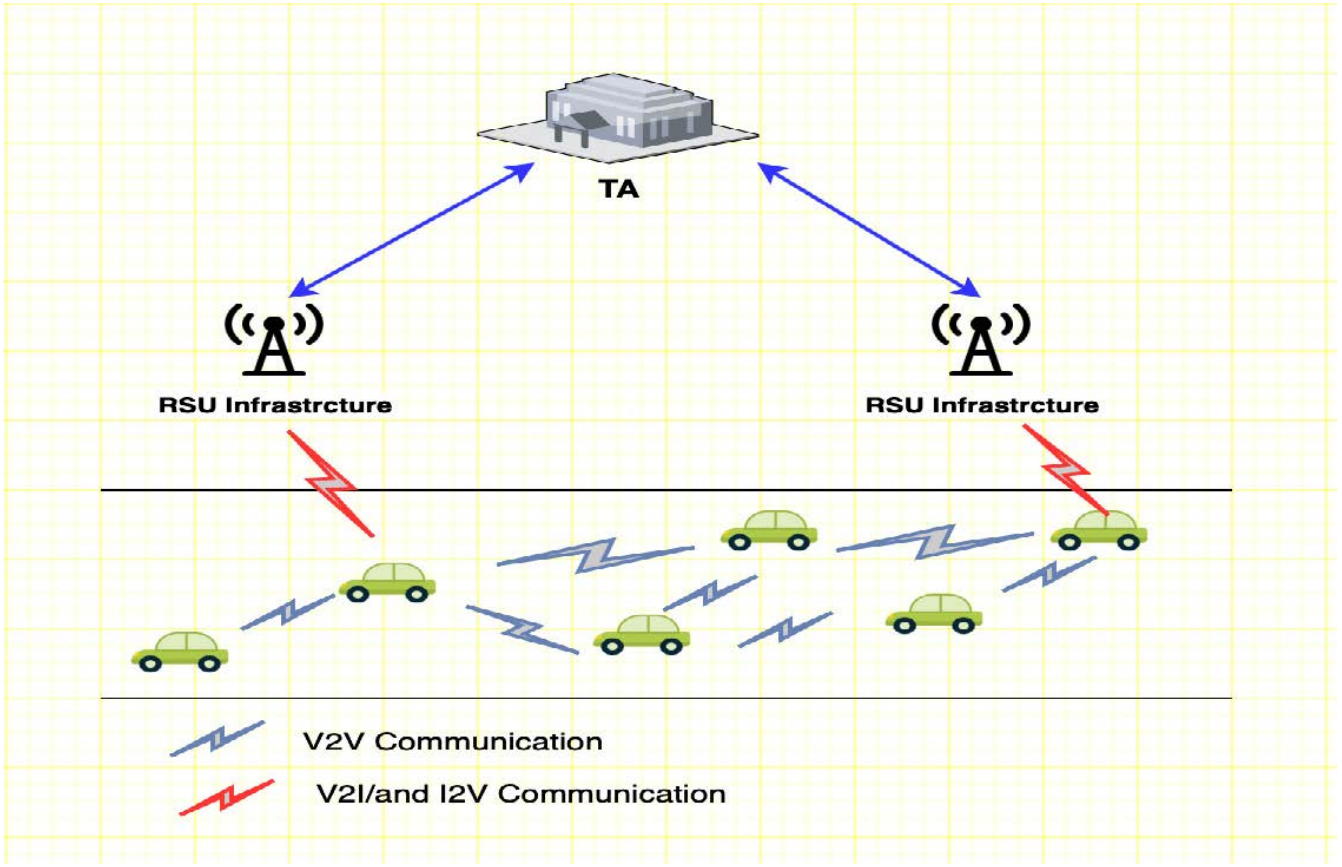

FIGURE 1. VANET architecture.

to provide safety for drivers, passengers, and pedestrians on the road. VANETs consist of three main components (see Fig. 1): the vehicle, road site unit (RSU) infrastructure, and traffic authority (TA) [8]. Each vehicle is equipped with an on board unit (OBU), which consists of various numbers of intelligent sensors that collect valuable vehicle and road status information, such as information on accidents and traffic jams and from surveillance of the city at night, to provide road safety for drivers, passengers, and pedestrians [9]. This collection of information is shared among the VANET components. VANETs consist of three communication links: V2V, in which the vehicle communicates directly with other vehicles; V2I or I2V, in which the vehicle communicates with the infrastructure or vice versa, respectively; and V2E, in which the vehicle communicates with everything on the road [8].

V2V, V2I, and V2E communicate by using the dedicated short-range communication (DSRC) protocol [10], WiMAX [11], fourth generation-long-term evolution (4G-LTE) [12], and 5G [13]. With the great advances in technology, sensors are now producing a mass of data, which are sometimes difficult for the OBU to process to make decisions in the real world. In addition, some of these data are highly sensitive and need to be secured from internal and external intruders. To overcome this limitation in the OBU, the vehicle can share the data by processing and storing data near the RSU to form a temporary cloud. A new concept was proposed in [14]. This concept focuses on integrating the VANET with cloud computing (CC) to form a new technology called vehicular cloud computing (VCC) to improve efficiency and traffic safety in the vehicular network. VCC is defined as autonomous vehicle groups that can exchange safety and non-safety data, storage, resources, sensing, communication, services, and application processing with authorized vehicles on the road and combine the resources of vehicles to form a cloud on the road.

The authors in [15] proposed a new service for VCC called platform as a service (PaaS). This service (PaaS) requires many resources if it is to be employed in complex real-time services and applications in VCC. Hussain *et al.* [16] proposed an approach to shift from a traditional vehicular network (VANET) to VCC. The authors explored the benefits of using VCC and demonstrated the communication flow between vehicles, RSUs, and cloud computing by using 4G-LTE. In addition, by combining traditional vehicular networks with CC, several types of applications and services that are difficult to apply in pure VANETs can be applied in VCC. One type involves using real-time video surveillance data to monitor drivers, pedestrians, and critical events in both urban and rural cities. Real-time video surveillance data

services may help governments, especially traffic authorities, monitor roads where there are no surveillance cameras (such as CCTV).

Some studies propose new surveillance services in VCC. In [17], the authors proposed a new service called picture-on-wheel (PoW). This approach aims to capture pictures or record a video on demand by using the camera of the vehicle. These videos and pictures are taken in passive mode and sent to the traffic authority in the cloud. However, some of these pictures or videos contain information that requires a preliminary decision about events from the authorities and may contain sensitive information, such as the vehicle's identity, the vehicle's location and sensitive video data, which should be protected from adversaries during transmission between entities in the vehicular network. Any modification, insertion, or sniffing of the information in the packet will affect decisions made by traffic authorities regarding to the event. However, this approach does not consider security and privacy issues.

In [18], data security and privacy among vehicles, RSUs, and clouds resulting from VCC were discussed. The authors outlined VCC challenges, such as high mobility authentication and scalability arising from the use of the DSRC protocol. However, the DSRC protocol affects the transfer of video data services between vehicles and authorities because of high latency. In [19], [20], the authors outlined that some factors will affect data transmission in the VCC environment; these factors include packet loss, high handover latency, and communication overhead. However, these factors should be considered when designing robust VCC architectures.

In VCC, real-time video surveillance data poses many security and privacy issues and challenges related to the authentication, integrity, confidentiality, availability, and privacy of the data as well as attracting new attacks, such as man-in-the-middle, quantum, Sybil, and artificial intelligence (AI) attacks [21]. When video data are being transmitted between vehicles, infrastructure, and clouds, these types of attacks should be addressed by implementing efficient security protocols. Moreover, in VCC, vehicles exchange real-time video surveillance data in an open access wireless environment; consequently, vehicles are more vulnerable to intruders in the network. In such an environment, intruders can intercept the packet and then modify, insert or delete the real-time video data that are exchanged among vehicles and infrastructures to communicate with a trusted entity in the VCC environment. Moreover, the intruder can record fake real-time video data, such as traffic jams, accidents and hazards, and then share it with trusted vehicles on the road, thereby affecting the performance of network. Therefore, to effectively apply real-time video surveillance data in the VCC domain, security and privacy should be handled by designing a powerful security protocol and introducing sophisticated cryptography algorithms to tackle all types of intruders and threats and achieve network efficiency, reliability, scalability, availability, ultra-low latency, and mobility, which are the main requirements when designing a new real-time video data system architecture. The main contributions of this study are as follows:

- First, we provide an overview of VANETs and some challenges related to storing many data in OBUs.
- We then provide an overview of VCC and its novel services and applications, such as real-time video-reporting services.
- Next, we explore the current research on VCC related to real-time video reporting services, determine the shortcomings of the research, discuss the security- and privacy-preserving aspects of video reporting in VCC, and discuss current solutions provided by researchers.
- We then present a new taxonomy of VCC related to real-time video data services.
- Next, we demonstrate the importance of 5G and 6G in real-time services and applications in VCC environments.
- Finally, we discuss the findings and present challenges and open issues in the VCC environment.

The remainder of this paper is structured as follows. The taxonomy of real-time video data in VCC is reviewed in Section II. Related work is presented in Section III. Our discussion and open issues are presented in Section IV, and conclusions and suggestions for future work are presented in Section V.

II. A TAXONOMY OF REAL-TIME VIDEO DATA IN VCC

This section provides a state-of-the-art taxonomy for real-time video data services in VCCs. This taxonomy comprises ad hoc networks, mobile ad hoc networks, VANETs, CC, and VCC. VCC is then expanded in detail, as shown in Fig. 2.

A. AD HOC NETWORK

The following section describes two main types of ad hoc networks: mobile ad hoc networks and vehicular ad hoc networks.

1) MOBILE AD HOC NETWORKS

Mobile ad hoc networks (MANETs) [22]–[24] are defined as a group of wireless devices, such as laptops, tablets, smartphones, and smart watches. These devices can communicate with each other to operate wireless networks. In MANETs, the wireless device can be an end user or router, which is called a multihop [25], [26]. Therefore, wireless local area networks (WLANs) and Bluetooth technology provide evidence of the use of MANETs in wireless networks.

2) VEHICULAR AD HOC NETWORK

A VANET is a type of MANET that provides wireless communication between vehicles that roam in a city. The vehicle uses the DSRC protocol, 4G-LTE, or 5G to communicate with other vehicles and RSUs. The DSRC protocol was based on 802.11a [27]. In addition, the vehicle could communicate with other vehicles in three ways. The first method is

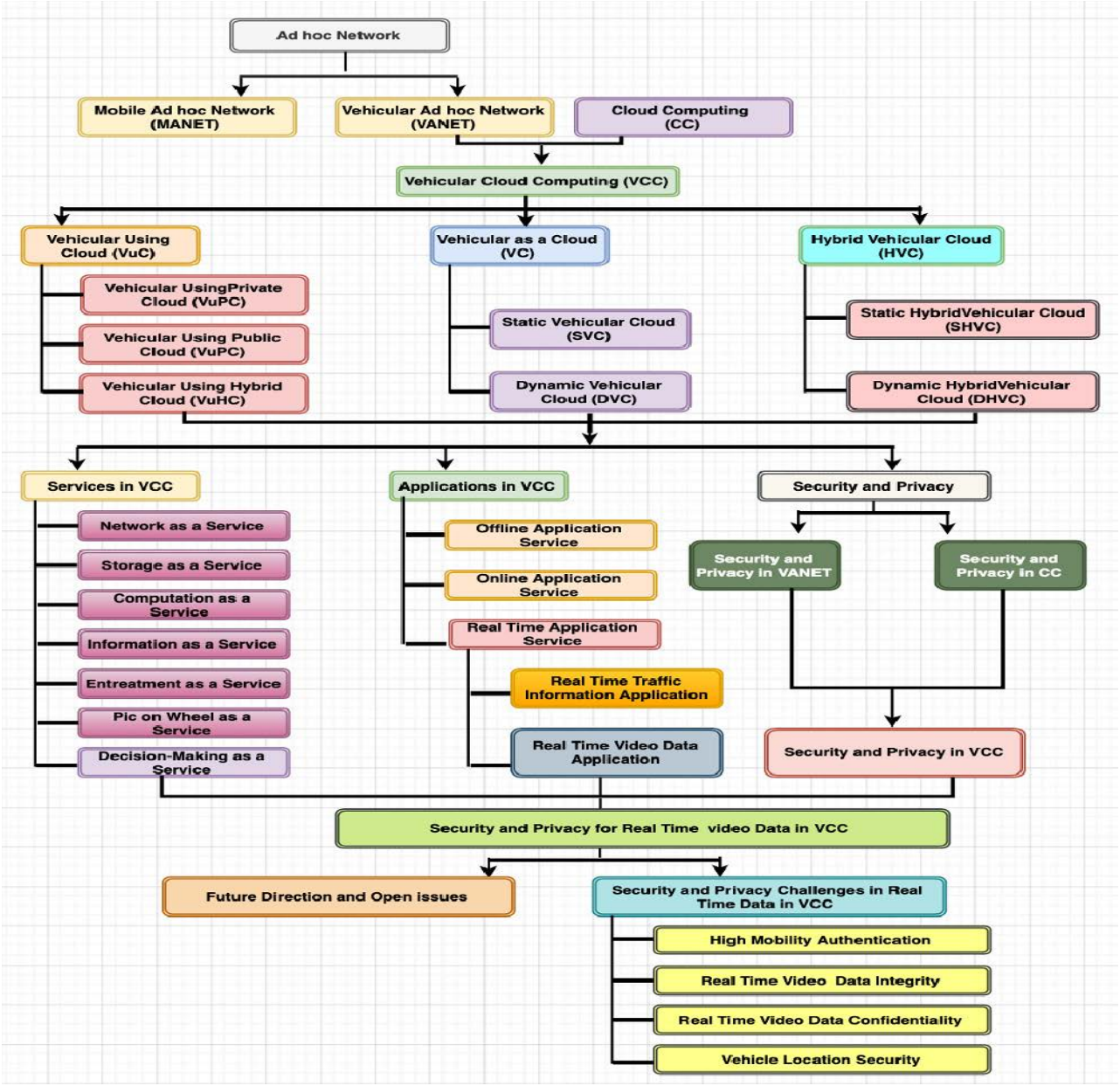

FIGURE 2. A taxonomy for real-time video data in VCC.

direct V2V communication. In the second method, the vehicle communicates with other vehicles via the RSU. In the third method, the vehicle communicates with everything. In addition, safety messages are shared among vehicles in one of the above ways to notify drivers of critical hazards or provide non-safety messages, such as weather and entertainment. The main aim of VANETs is to provide traffic safety for drivers and passengers to avoid accidents and traffic jams on the road.

In-Vehicle Devices. A vehicle consists of three elements: an OBU, an application unit, and a tamperproof device.

1. **OBU:** Each vehicle is equipped with an OBU The OBU is responsible for communication with other vehicles and RSUs. In addition, the OBU contains a resource-computer processor (RCP). The RCP device is responsible for processing the safety and non-safety messages received by vehicles. This processing information is sent from one OBU to another OBU in different vehicles [28].
2. **An application unit (AU)** is a device that is considered a physical unit similar to an OBU [29]. The AU uses the OBU to run applications through the internet. In addition, an AU consists of a personal digital assistant (PDA) or any device dedicated to safety applications. The AU can use wire or wireless communication with the OBU.
3. **Tamperproof Device (TPD):** A device in the OBU that protects vehicle information, the TPD stores private

and public keys for long- or short-term communication between vehicles and RSUs [30]. In addition, the TPD is responsible for encrypting and decrypting data, which transfer among vehicles and RSUs through the OBU. TPD can be accessed only by authorized users, such as traffic authorities. According to encrypting and decrypting messages in the TPD, the keys have a lifetime to expire, and then they are stored in the TPD after expiration. However, this process causes overhead in the TPD, which cannot process the message quickly, especially for real-time services and applications that require a high-priority process. Therefore, the TPD should have a mechanism to delete expired keys and certificates.

B. CLOUD COMPUTING

Cloud computing (CC) [31], [32] is a new technology that provides powerful computation, storage, processing, resources, and application services. The main aim of CC is to provide services to the end user anytime and anywhere. In addition, organizations and enterprises have shifted to cloud technology to upload their resources and access these resources through the internet to reduce maintenance costs. The architecture of CC has many datacenters that are responsible for user requests and processing these requests quickly. CC comprises three types of clouds [33]. The first type is the public cloud, which is used by all users around the world; examples include Google Drive and Amazon. Data in the public cloud should be highly protected against adversaries. The second type is a private cloud, in which each user or organization creates its own cloud. The third type is a hybrid cloud, consisting of public and private clouds. Moreover, cloud computing has three modeling services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [34].

C. VEHICULAR CLOUD COMPUTING

VCC [35]–[38] is a new technology formed from a combination of a VANET and CC. VCC is defined as ''a group of largely autonomous vehicles whose computing, sensing, communication, physical resources can be coordinated and dynamically allocated to the authorized users'' [14]. The main aim of VCC is to enable vehicles to share, process, sense, and compute complex real-time video surveillance data with other vehicles through the cloud. Additionally, VCC provides new services and applications that are difficult to implement in VANETs. The challenges that occur when connecting vehicles to form a VCC are similar to those faced in VANETs [39] and CC [40] because VCC is a combination of these two technologies. Consequently, VCC and VANET can be utilized to solve issues in ITS. In [15], the authors proposed three main types of VCC. These types are vehicular using cloud (VuC), vehicular as a cloud (VC), and hybrid vehicular cloud (HVC).

1) VEHICULAR USING CLOUD

The VuC uses the OBU to collect and share safety messages, such as regarding street status, driver status, and traffic jams, among vehicles and clouds through the RSUs or directly to the cloud (see Fig. 3). First, the data that are collected by the vehicle's sensors are first processed in the OBU; then, the OBU sends a copy of the data to the traffic authority in the central remote cloud for storing and making a decision in the real world.

In addition, the OBU collects driver and passenger data from devices, such as smart phones, smart watches, and tablets, that are connected to the OBU via the internet. Some of these data contain sensitive information that requires a quick decision in real time; making a quick decision requires high bandwidth and low latency between vehicles and the remote cloud. As a result, there are three types of VuC: vehicles using private cloud, vehicles using public clouds, and vehicles using hybrid clouds.

1- Vehicles using a private cloud (VuPCs): A VuPC is responsible for creating a private cloud on the road by the traffic authority. VuPCs can be accessed only by police vehicles to download and upload data to the cloud. The main aim of VuPCs is to reduce the overhead on public traffic authorities and provide information to police officers.
2- Vehicles using a public cloud (VuPuCs): Each vehicle should be registered with the traffic authority before starting to record any events on the road. Registration depends on the security requirements for maintaining traffic safety on the road. After registration is completed, a new identity is assigned to the vehicle to start recording and sharing any events in the city with the traffic authority.
3- Vehicles using a hybrid cloud (VuHCs): A VuHC is a combination of a VuPC and a VuPuC. A VuHC can be a police vehicle or a trusted vehicle that works with the government.

2) VEHICULAR AS A CLOUD

A VC is responsible for creating a cloud for a group of vehicles on the road (see Fig. 4). In the VC scenario, the vehicle sends an invitation message to neighboring vehicles on the road to join its cloud via the DSRC protocol, 4G-LTE, or 5G. The vehicles that receive the invitation should reply ''yes'' or ''no.'' If any vehicle replies ''yes,'' then the concept of the VC is achieved. Vehicles in a VC are called vehicle members. These members should elect one vehicle to be a master in the VC to receive, process, and compute the messages that are received from one of the vehicle's members and then forward the message to all vehicles in the VC. The main benefit of VCs is that they create a local data center and reduce overhead on the cloud. In addition, there are two scenarios of VCs: static and dynamic. A static VC is a group of vehicles in static mode, such as parked at an airport, while the dynamic

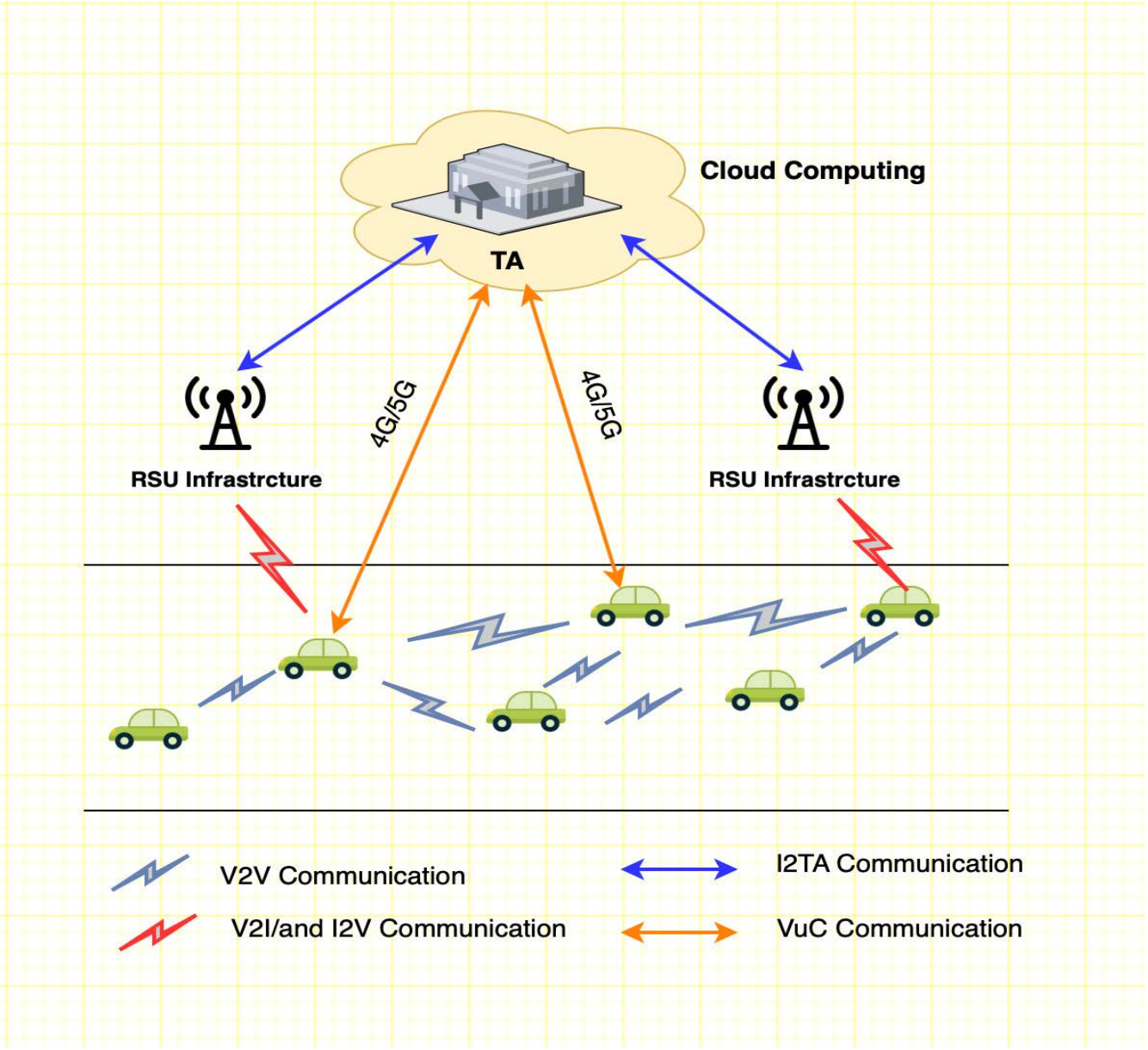

FIGURE 3. VuC architecture.

VC is moving on the road. For example, friends who travel on the road create a dynamic VC to exchange entrainment information.

3) HYBRID VEHICULAR CLOUD

A HVC is a combination of a VC and a VuC; consequently, vehicles can join the VC as a service provider, and they can also access the internet cloud to use cloud services via gateways, such as RSUs/vehicles (see Fig. 5). There are two types of HVCs: static and dynamic. Therefore, HVC inherits all the advantages and disadvantages of VuCs and VCs.

D. SERVICES IN VCC

In this section, we provide an overview of VCC services [20]: network as a service, storage as a service, computation as a service, information as a service, entertainment as a service, and picture on wheel as a service. In addition, a new service, called decision as a service, is presented for real-time services and applications.

1) NETWORK AS A SERVICE IN VCC

As mentioned previously, RSUs and mobile vehicles can create a network as a service (NaaS) on the road. Some of

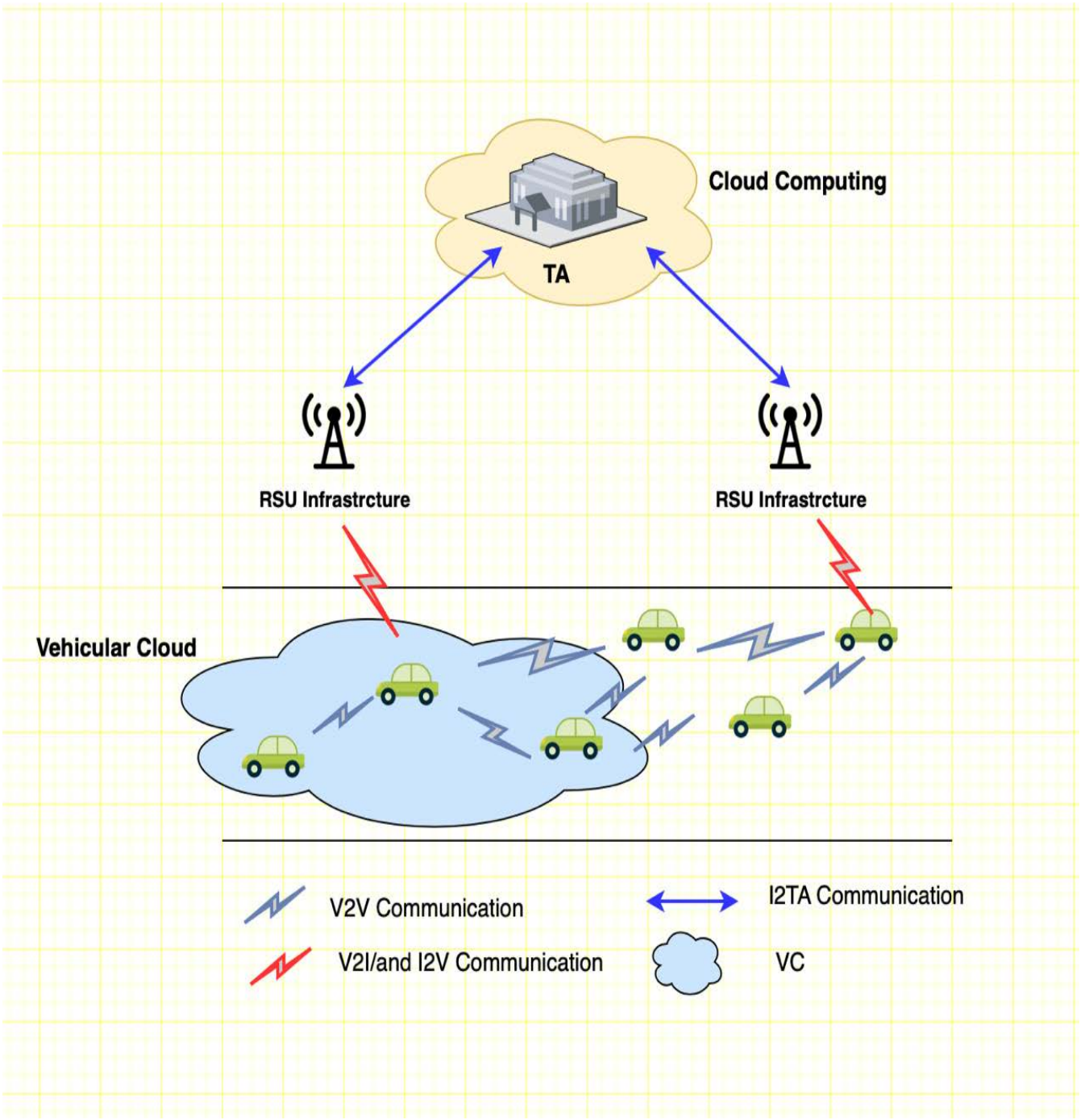

FIGURE 4. VC architecture.

these vehicles can access the internet via DSRC, WIMAX, Bluetooth, 4G-LTE, 5G, or 6G (in the future) [41] while traveling on the road. In addition, RSUs and vehicles (such as vehicles parked at a mall) can act as a type of mobile gateway for other vehicles on the road to exchange safety and non-safety messages among vehicles that have connections with the internet. Therefore, NaaS provided by vehicles or RSUs can be paid or free.

2) STORAGE AS A SERVICE IN VCC

Each vehicle is equipped with an OBU. Each OBU consists of various numbers of sensors that collect data from inside and outside the vehicle; the data are then stored in the OBU. The OBU consists of two units: a processing unit and a communication unit [42]. The main aims of the OBU are the processing, computation, and storage of data collected by the OBU sensors. Moreover, the OBUs in old vehicles

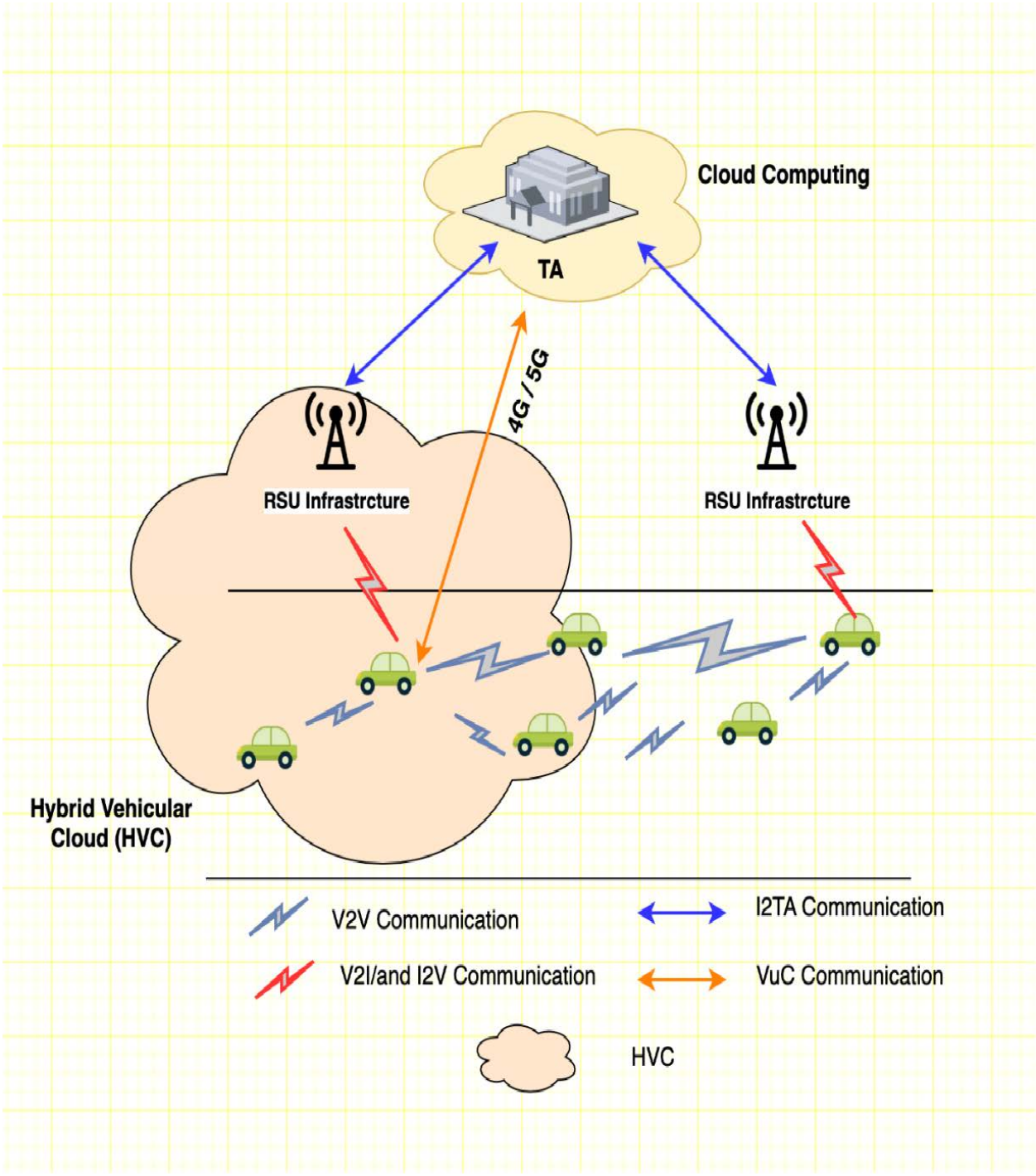

FIGURE 5. HVC architecture.

have limited storage, whereas modern vehicles are equipped with a high storage capacity. For example, Tesla [43] and Lucid [44] are self-driving electric vehicles that do not have traditional vehicular machinery; these vehicles' companies take advantage of this feature by providing high-performance computers and high-capacity storage to help other vehicles make decisions during transportation on the road and by providing storage as a service (SaaS) for other vehicles. For example, if the vehicle stops in the airport parking for a long time and has a high storage capacity, the vehicle will provide SaaS services for other vehicles around the airport, either for a fee or paid service.

3) COMPUTATION AS A SERVICE IN VCC

A smart vehicle can provide computing as a service (CoaaS) for other vehicles on the road. In the future, a smart vehicle, especially electric vehicles, may possess the same computing capabilities as a personal computer [43], [44] because the machinery of an electric vehicle is not similar to that of a traditional vehicle. In addition, the OBU can employ this computing power to perform data processing tasks. Thus, CoaaS can be rented to authorized vehicles when they are not in demand by the vehicle's drivers. For example, a vehicle may be stationary in a vehicle park. In this case, complex computations that require considerable processing power could be handled by the aggregated resources of several vehicles; such power would not be possible with a single vehicle. For such computations to operate efficiently, high-level mechanisms for task scheduling are required.

4) INFORMATION AS A SERVICE IN VCC

Autonomous vehicles store the data gathered by using advanced OBU sensors. In VCC, vehicles can store data, such as weather data, environmental (e.g., Earth quick) data, traffic information, weather information, traffic accident information, audio, video, and pictures, which are collected from sensors in vehicles or RSUs. The information as a service (INaaS) provider, who, in effect, rents the resources from the owner of the vehicle, can then utilize these data to answer queries sent in by other vehicles.

5) ENTERTAINMENT AS A SERVICE IN VCC

Many people are expected to have entertainment options in their vehicles as they travel. This service would enable drivers and passengers to enjoy movies, videos, and advertisements while they are travelling, thus making the journey more enjoyable and comfortable by using Apple car play [45] and Android auto [46].

6) PICTURE-ON-WHEEL AS A SERVICE IN VCC

The authors in [17] described POWs in VCC where vehicle cameras can be used to send images to drivers and passengers or to send images of critical events on the road to the traffic authority. POWs may be useful for real-time application services because the mobility of vehicles can be used to widen coverage beyond what is possible with static sensors. Although mobile phones can be utilized for this service, they have constraints on battery life, and the information stored on a mobile phone may not be completely secure. Owing to the advantages of VCC, POWs do not have issues with power consumption. A POW uses an appropriately selected group of vehicles to take photographs or videos to capture the traffic or weather situations requested by a customer. A POW also gives the government a better picture of the situation in cities by monitoring them and providing clear data about activities and events, such as vehicle accidents, criminal activity, and fire. To handle this service, vehicles need to register with the traffic authority in the cloud to access the POW service.

7) DECISION-MAKING AS A SERVICE IN VCC

Decision-making as a service (DMaaS) is suitable for real-time application services that require preliminary decisions regarding to the events on the road. This service requires high bandwidth among vehicles, RSUs, and traffic authorities to make decisions quickly because any delay in decision-making may affect the driver's or passenger's life or may cause a traffic jam on the road.

E. APPLICATIONS IN VCC

In this section, there are three types of applications: offline, online, and real-time; all require fast decisions from the traffic authority department. The following subsections describe these applications.

1) OFFLINE APPLICATIONS IN VCC

The offline application collects data from inside a vehicle. The data are collected using OBU sensors, such as oil sensors, temperature sensors, tire sensors, break sensors, and gasoline sensors [14]. The collected data are then stored in the OBU; the data do not need to be uploaded to the cloud. The main purpose of offline applications is to help vehicle companies know the exact details of their vehicles in the event of a factory defect and find the right ways to solve the defect.

2) ONLINE APPLICATIONS IN VCC

The online applications are responsible for collecting real-time data from inside and outside vehicles; such data include data on the city status at night, traffic jams, weather, and driver status inside the vehicle [19]. In addition, there is a vast amount of online application data collected and they are not sufficiently stored in the OBU because of the limited storage of OBUs. To solve this issue, online application data are uploaded to the cloud via the vehicle directly or by RSUs. However, this type of data does not require a real-time decision to improve road traffic.

3) REAL-TIME APPLICATIONS IN VCC

Real-time applications are responsible for collecting sensitive information in real-time from the road (see Fig. 6). For instance, when a vehicle is roaming on a road, it is possible to record urgent events, such as fires, traffic accidents, earthquakes, flooding, and tornadoes, by using the vehicle's camera. The OBU then transmits this data to the TA in the cloud directly or via the RSU. Then, the TA should make a decision about the data that is received in real time to notify the police officer to attend to the event's location. In [47], the authors proposed a new idea for distributing digital advertisements in real-time. The idea is to choose particular public vehicles, such as taxis and buses, to distribute advertisements among vehicles on the road. However, this approach has some limitations: 1) this approach causes an overhead on the OBU because the vehicle can receive a multiple of the same digital advertisement at the same time; and 2) the vehicles do not know if this advertisement comes

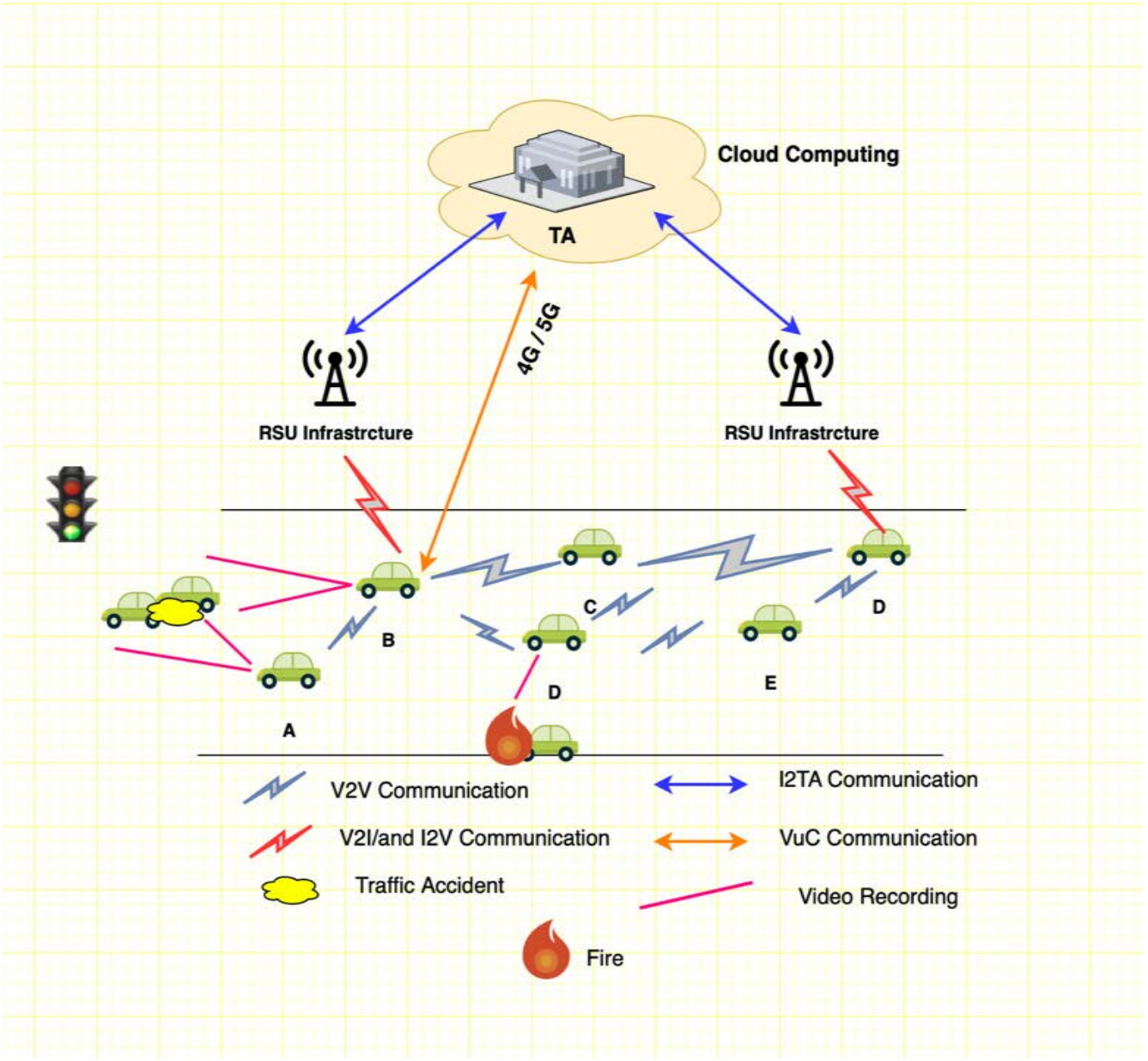

FIGURE 6. Recording critical events on the road.

from authorize/unauthorized vehicles. Therefore, all these application services will generate many data that are difficult to store in OBUs because of OBUs' limited storage.

a: REAL-TIME VIDEO SURVEILLANCE DATA IN VCC

Providing real-time video surveillance data in urban and rural cities is one of the most important services in VCC because this service helps governments and law enforcement agencies (authorities) track people and vehicles by using CCTV or high-definition (HD) video to ensure security and safety. Authorities need to respond quickly to events as the events occur, and as a large storage space is required for processing HD videos in real time, VCC is an ideal option. HD videos of public transport will produce massive data when public transport is roaming between cities. Thus, vehicles and RSUs can be employed to quickly share information with relevant authorities so that actions can be taken in real time.

III. RELATED WORK

The real-time video data collected by the vehicle's camera on the road consist of sensitive information and the vehicle's identity, event type, event location, traffic authority's identity, and traffic authority's location; all this information should be protected from intruders during transmission through the network. Security and privacy are both crucial aspects, particularly for real-time video surveillance data services and

mobility, scalability, availability, and low latency in VCC environments. The VCC inherits the security and privacy issues of VANET and cloud computing. In this section, we explore the security and privacy of real-time video surveillance data services in VCC in four subsections: security and privacy in VANETs, security and privacy in VCC, and security and privacy for real-time video data services in VCC based on 5G and 6G.

A. SECURITY AND PRIVACY IN VANET

Vehicles communicate with each other to exchange safety and non-safety messages to avoid accidents and traffic congestion in modern and rural cities. These messages contain sensitive information that is at risk if they are not protected from unauthorized nodes (e.g., malicious vehicles). Therefore, security and privacy are mandatory for protecting safety messages and vehicle identities from adversaries.

Several studies [48]–[53] have presented comprehensive reviews on overcoming the security and privacy problems in VANETs. These studies aimed to demonstrate the importance of securing and protecting the data transferred between vehicles and of securing and protecting the identities of vehicles from adversaries by designing effective security protocols. The authors of [54] proposed the following stand-alone security requirements for VANETs: integrity, confidentiality, authentication, user and location privacy, nonrepudiation, and conditional anonymity. Several methods have been used to secure communication in VANETs; these methods include pseudonyms, group signatures, and identity-based encryption. In [55], the authors outlined the security and privacy requirements of VANETs. These requirements include confidentiality, nonrepudiation, privacy protection, and control access. Raya *et al.* [56] identified the following threats faced by VANETs: impersonation, forgery, replay, and jamming. The threats facing VANETs can be divided into three main categories: authentication, availability, and confidentiality [57].

In VANETs, a certificate authority (CA) is used for vehicle authentication. If any vehicle is compromised by adversaries, the certificate of the compromised vehicle is revoked and sent to the certificate revocation list (CRL), which is distributed to all legitimate vehicles, to prevent the exchange of any safety or non-safety messages with the revoked vehicle. The distribution of the CRL to all nodes (vehicles) without distortion is vital to securing communication in VANETs. The RSU handles the distribution of the CRL to all vehicles and tracks misbehaving vehicles. Legitimate vehicles cannot obtain a CRL if they move out of the RSU range. Therefore, RSUs should be deployed appropriately along the road; however, this deployment may incur a high cost.

The authors of [58] proposed an efficient method to overcome the use of a limited number of RSUs on the road. The authors aimed to use vehicular nodes to distribute the CRL when there was no RSU at the legitimate vehicle's location. The proposed simulation demonstrated that the distribution of a CRL through vehicular nodes can outperform the use of RSUs. However, the authors' method places a heavy load on legitimate vehicle OBUs by sending frequent broadcasts through vehicular nodes.

In a VANET, each vehicle is equipped with an OBU device that stores the CRL and exchanges information among vehicles for safety and non-safety applications. However, an OBU cannot process complex data, particularly data that require real-time decisions. Therefore, researchers have considered the benefits and advantages of VANET and CC and proposed VCC.

B. SECURITY AND PRIVACY IN VCC

The authors of [14], [59] proposed a new concept, VCC, by integrating CC with VANETs. This integration allows autonomous and intelligent vehicles to manage new services and applications, especially in real time. Such vehicles collect real-time data from the road; store the data in the vehicles' OBUs; and share the data among vehicles, RSUs and traffic authorities in real time.

In [18], the authors outlined VCC security and privacy challenges, such as high-mobility authentication, which may affect the passing of real-time video data between vehicles and infrastructure. However, security and privacy solutions have not yet been mentioned.

Similarly, the authors in [19], [20] pointed out the main issues of security and privacy in VCC. The authors provided some parameters that may play an important role in designing a security architecture for VCC; these parameters include high handover latency, packet loss, and communication overhead. However, the solutions for security and privacy issues are not addressed.

In [59], the authors presented a new mechanism by integrating VCC with a cyber physical system. The main objective of this integration was to monitor drivers while moving in the city. The study methodology is based on using a driver body sensor (DBS) that reads vital body reactions and sends the data to the OBU of the vehicle through wireless communication. Nevertheless, the main security and privacy challenges and issues have not yet been addressed

The author of [60] presented a new architecture for VCC. This architecture consists of three-tiers: the vehicular cloud, the RSU, and CC. Additionally, the author mentioned the security requirements and threats of the proposed architectures. However, this study does not provide any security or privacy solutions and does not show how data are transferred among tiers. In [61], the authors presented a new hierarchical architecture for VCC. This study shows how communication is performed among entities in their proposed architecture, but security and privacy were not considered.

Wan *et al.* [62] presented a new approach called VCMIA, in which a vehicular cyber physical system (VCPS) is integrated with mobile cloud computing (MCC) to support a cloud provider and an ITS. The main objective of this approach is to enable users to access the central cloud and share information between the cloud provider and the vehicle. Similarly, a new approach is presented by the authors in [63].

This approach is VCPS, which integrated a VCPS with the communication between the mobile user and cloud provider. Although the authors in [62] and [63] mentioned security challenges, they did not present any solutions.

The researchers in [64] presented a new security mechanism in which location-based encryption is used to protect the confidentiality of location from external intruders. In this study, the vehicle changes its key when roaming among zones on the road. To exchange the information, the source vehicle and receiver of the vehicle should be located in the same zone. Nevertheless, a limitation of this approach is that communication is lost when both sender and receiver are located in different zones.

Mershad and Artail [65] proposed a new system called CROWN, which uses RSUs as cloud interfaces and directories. In the CROWN system, vehicles can access data covered by the RSUs; however, these vehicles cannot access data outside the RSU range.

Park *et al.* [66] proposed a privacy-preserving scheme for protecting vehicles and infrastructure in a vehicular-based cloud. The authors presented a new architecture that consists of a master authority, transportation manager, and server manager. The vehicle's OBU generates the vehicle's pseudonymous certificate and sends the certificate, along with vehicle's real identity, to the master authority. However, the proposed architecture does not work well if no RSU is located in the vehicle location.

Hussain *et al.* [67] proposed a new security protocol for securing traffic information. This study made two assumptions: the first assumption is that each zone is covered by three RSUs, while the second assumption is that the vehicles are authenticated to obtain a symmetric key zone (i.e., a Kzone), which is distributed by the RSU when a vehicle joins a new zone. However, this approach suffers from overhead on the vehicle's OBU.

Nkenyereye and Rhee [68] proposed a new security protocol for securing traffic management in VuC [16]. The objective of the security protocol is to secure data traffic transmission between transportation centers and vehicles through RSUs by using an identity-based digital signature (IDS) scheme. However, the packets that are transmitted between RSUs and the transportation center through the network is easily intercepted and modified by an intruder.

Kang *et al.* [69] presented a new approach that is a service-oriented security method for VCC. This approach provides two new services: payment and accident management. The main aim of the accident management service is to monitor the driver by using human body detection, such as by using a camera inside the vehicle, whereas the payment service aims to purchase goods online through the dashboard console of the vehicle. This study outlined various security requirements, such as integrity, availability, confidentiality, and privacy protection. However, vehicle communication is disconnected from the central cloud if the vehicle is outside the RSU coverage.

The authors of [70] provided a new vehicle architecture based on fog computing techniques. This architecture consists of three layers: the vehicle, fog, and CC layers. The vehicle layer handles the transmission of data to the fog layer. The fog layer consists of RSUs, base stations, computing resources, resource storage, and a local authority (LA). The LA is responsible for generating pseudonymous certificates for vehicles. Moreover, the authors assumed that the fog layer could be trusted. The CC layer is responsible for storing the data that are uploaded by the fog layer; however, the security and privacy of communication channels between the fog and cloud layers are not considered.

Garai *et al.* [71] proposed a new mechanism for distributing keys and manage the mechanism between vehicles, RSUs, and the central cloud according to the VCC concept that is presented in [16]. This mechanism is a certificate-based privacy and authentication protection protocol. The main objective of this study was to prevent Sybil and tracking attacks. In addition, the architecture proposed in this study consists of three layers: a central cloud, RSU cloudlet, and vehicle cloudlet. The RSU cloudlet and vehicle cloudlet communicate with each other since the vehicle cloudlet receives messages from its members and forwards the messages to the RSU cloudlet. Additionally, the vehicles need to change their certificates when roaming between different RSUs to support intra- and inter-RSU cloudlets. However, the intruders can modify and intercept vehicle information when roaming among RSU cloudlets.

The authors of [72] proposed a new mechanism for selecting cluster heads in VANETs by using fuzzy logic based on cognitive radio (CR). The authors used two types of fuzzy logic: fuzzy input for CR VANET and fuzzy to noise. Moreover, the authors explore the three main parameters for creating a cluster on the road: cluster head (CH), cluster member (CM), and cluster gateway (CG). This work is extended in [73]. Although this study presents an important technique in VANET, which is a cluster, this study did not mention the security and privacy of real-time data in VCC.

The author in [74] proposed a comprehensive survey of VANET clouds. In this survey, the authors started by introducing a new architecture and new applications and the main challenges and open issues. However, the authors did not mention the security and privacy solutions of real-time services in VANET clouds.

Whaiduzzaman *et al.* [20] presented novel services, such as storage as a service, traffic information as a service, computation as a service, network as a service, and entertainment as a service, by combining VANETs with CC. VCC is consider as a suitable environment for generating new real-time services for monitoring road events and can draw a clear picture for local authorities to understand. Nevertheless, these real-time services generate many data that must be rapidly transmitted among network entities with low latency.

The 4G-LTE and DSRC protocols are insufficient for transmitting real-time data in VCC because these protocols suffer

from delays and lack of scalability, respectively. Thus, 5G technology is considered promising for transmitting real-time video reporting data in VCC. These services may contain sensitive information that should be protected against attacks.

C. SECURITY AND PRIVACY FOR REAL-TIME VIDEO DATA SERVICES IN VCC BASED ON 5G

Security and privacy are one of the issues and challenges in 5G networks because the data rate transmission among entities is faster in 5G networks than in 4G-LTE technology. 5G networks can facilitate the adoption of technologies, such as device-to-device (D2D) communication, software-defined networks (SDNs), and network function virtualization (NFV). Each of these technologies has unique security and privacy challenges and issues. Several studies have explained the importance of security and privacy in 5G environments [75]–[78]. Mantas *et al.* [79] outlined the possible threats and attackers against the main entities of 5G networks. These attacks and threats were derived from 3G, 4G, and 4G-LTE networks to identify the security challenges and issues in 5G networks. In addition, the 5G architecture consists of user equipment, external internet protocols (IPs), access networks, and the core network of the mobile operator. However, the main security and privacy issues in D2D communication have not been mentioned.

Alam *et al.* [80] proposed a new protocol for securing D2D communications in LTE-A networks. The authors presented three network scenarios for analyzing possible threats in D2D communication: D2D in public safety, D2D without user applications, and D2D with user applications. Therefore, this study did not mention threats to real-time services and applications, although the authors identified threats in such applications.

The author of [81] presented a comprehensive survey of D2D communication. The authors begin by giving an overview of the D2D communication concept in three different respects: communication scenarios, status, and the advantages of D2D communication in public safety applications. However, solutions for security and privacy issues were not addressed.

A new protocol for providing a group authentication in D2D communication is presented by the authors in [82]. This study is based on the works in [83] and 3GPP 23.023 [84] and used hybrid techniques, such as Diffie–Hellman (DH) key exchange [85], an authentication encryption standard (AES-128 bit) [86], aggregated signatures [87], and elliptic curve cryptography (ECC) [88], to achieve the following security requirements: integrity, confidentiality, and authentication against intruders. The main objective of this study is to implement a group device leader for reducing the communication overhead. Nevertheless, the protocol proposed in this study has not been applied to an HVC environment.

The authors of [89] extended the work in [90]. The authors used a new VANET-based mechanism is called MobEyes for urban monitoring. This study is considered a pioneering paper on urban monitoring, as this study describes the use of MobEyes to assist in opportunistic diffusion. MobEyes is based on vehicle sensors that collect data from inside the vehicle and from the surrounding vehicle environment; the sensors then forward the data to other vehicles through one hop or multiple hops. The paper shows the two most common types of urban monitoring: infrastructure communication and static sensor deployment. Therefore, a further investigation of security and privacy aspects is required, although this study provides a simple security mechanism by using a simple one-way hash function and asymmetric cryptography without details.

A new approach for monitoring truck drivers by using multiple cameras inside a vehicle is presented by Kutila in [91]. Similarly, the authors of [92] proposed a new mechanism for monitoring drivers in vehicles. The proposed mechanism used a new technique called a spatiotemporal technique. A spatiotemporal technique is used for two purposes: first, to make momentary decisions about various events, and second, to classify the driver distribution level. Nevertheless, neither [91] nor [92] addressed security and privacy issues.

Weng [93] presented two types of surveillance services. The first service is called the forensic picture service, in which a vehicle can provide an offline picture by making the picture available before requesting it from the customer; the second type is called the photo-shooting service, which allows users to provide a landscape photo. Similarly, Habtie [94] proposed a surveillance service for traffic monitoring and management by integrating cellular networks with CC. The proposed service was based on two methods, namely, conventional road monitoring and traffic accident statistics. However, the security and privacy issues are not considered by the above studies [93] and [94].

The authors in [95] proposed a new POW service. This service aims to monitor cities by using the vehicle's camera sensor. The vehicle's camera captures a photo or records video for events that occur on the road and forwards the photo or video to the nearest traffic authorities for decision-making; however, this study did not consider the security and privacy issues of the proposed service.

Hussain *et al.* [96] proposed a new service that is called vehicle witnesses as a service in VCC. The WaaS enables vehicles to capture pictures and to forward the pictures to law enforcement via the cloud by using the vehicle's camera. This study focuses only on a passive service that takes only an offline picture of the event after the event occurs on the road. To secure the picture, this proposal uses two security techniques, namely, ElGamal encryption [97] and ECC. Nevertheless, the intruders can easily obtain the pseudonyms of vehicles because the communication channels between the vehicles and trusted vehicles are not secure.

Eiza *et al.* [98] proposed the system architecture for a new surveillance service for monitoring traffic accidents in the city. This system architecture is based on a 5G network and CC. The proposed service aims to protect video data that are sent from participating vehicles to the central cloud. The authors used several techniques, including pseudonym

authentication, a threshold scheme based on a secret key, public keys with keyword search (PK-KS), and cipher policy attribute-based encryption (CP-ABE). The proposed service suffers from high latency when sending video data to the central cloud and download the data from the central cloud because of the long distance between the participating vehicle and the central cloud.

Nkenyereye *et al.* [99] proposed a new protocol for overcoming the weaknesses of the service proposed by Eiza *et al.* [98]. To deal with video data when transmitting among participating vehicles and the central cloud, Nkenyereye *et al.'s* approach consists of three layers: the remote cloud layer, the RSU infrastructure layer, and the vehicle layer. Compared with [98], this approach reduced the communication cost by 50%. Nevertheless, this approach suffers from an increasing communication overhead.

Almusaylim *et al.* [100] presented a new 5G network–based protocol for protecting data privacy in VCC. The main objective of this study is to improve the security of [99]. However, the security and privacy solutions were not considered.

Yoo [101] proposed a new protocol for securing video reporting services in a vehicular network by using D2D communications. The main objective of this approach is to overcome the limitations in [98] by extending the functionality of the remote cloud, the law enforcement agency (LEA), the TA, and DMV. This study used hybrid techniques, such as public key encryption with keywords, CP-ABE, and pseudonymous authentication, to secure the proposed protocol. However, the communication channels among the participating vehicles and TA are not secure.

Similarly, the authors of [102] presented a new mechanism for securing a video reporting service in a VANET based on a 5G network. The objective of this study is to overcome the limitations of [98]; these limitations include replay, fabrication, and denial of service attacks. In addition, the methodology of this proposed mechanism is to generate 730 pseudonymous certificates for each participating vehicle to use the pseudonymous certificates when recording any event on the road. Nevertheless, the intruders can easily intercept, modify, and insert false information in the packet among the TA and participating vehicles. Table 1 compares the advantages and weaknesses of the existing proposed solutions to ensure the security and privacy of video data in VCC. Table 2 presents the security techniques that are used in the literature to secure video data while data are being transmitted among entities in the network.

D. SECURITY AND PRIVACY FOR REAL-TIME VIDEO DATA SERVICES IN VCC BASED ON 6G

Although some countries have started implementing 5G networks that will revolutionize the world of wireless communication, researchers have begun to consider the specifications and features of sixth generation (6G) networks. Undoubtedly, this generation will entail considerable changes in networks involving AI communication among smart devices to exchange data in real time. The world's first 6G flagship program was launched by Oulu University, Finland, with a complete adoption planned by the beginning of 2030 [103]. Compared to its 5G counterpart, 6G technology will offer more interesting features, such as ultra-high ''seven-nines'' reliability, ultra-low latency, and ultra-high mobility for autonomous driving. The main motivations for focusing on 6G technology involve latency, data security, and privacy issues with 5G, especially for real-time services, thereby limiting the support for 5G technology.

Several studies have focused on 6G technology. Yastrebova *et al.* [104] proposed that the main challenges pertaining to such applications can be resolved by implementing 6G networks. Huang *et al.* [41] conducted a comprehensive survey of 6G technology and demonstrated the advantages of using 6G technology when compared to 5G. However, the security and privacy of 6G networks have not yet been addressed.

Aazhang *et al.* [105] presented a survey to identify the challenges posed by 6G networks. The authors' study focused on several potential 6G technology applications, such as unmanned aerial vehicles (UAVs), satellites and terahertz-enabled wireless communications. However, the authors did not consider the security and privacy issues of real-time services in vehicular networks.

A comprehensive survey of 6G technology was presented by Strinati *et al.* [106]. The authors began by providing an overview of 5G technology and the reasons for the requirements of 6G networks. The authors presented the main challenges of using 6G technology. Nevertheless, the authors did not consider the security and privacy issues and challenges.

Zhang *et al.* [107] presented key technological challenges for 6G technology applications. They explained how 6G can support the super Internet of Things (IOTs) and AI systems. Nevertheless, data security and privacy, which are the primary concerns associated with the design and use of any new technology, were not mentioned. In [108], the authors presented a comprehensive survey on the use of AI in 6G technology. The authors explored the importance of using AI in 6G and how 6G can be implemented in different ranges of applications, such as surveillance applications and ITS. This paper shows the differences among 1G, 2G, 4G, 5G, and 6G technologies and outlines why 6G technology is better. A new heterogeneous architecture is presented that consists of a physical layer, a data link layer, a network layer, and an application layer. However, this study does not provide solutions for protecting surveillance data service from adversaries while transmitting data among entities.

In contrast, Loven *et al.* [109] proposed a new 5G model that could be applied to 6G technology. This model comprises two parts: AI for edge computing and edge computing for AI. Edge AI can support novel applications, such as smart cities, urban computing, smart buildings, and self-driving. However, security and privacy issues and the corresponding solutions are not considered.

TABLE 1. A comparison of related works based on advantages and weaknesses.

Ref	Advantages	Weaknesses
[17]	The study proposes a new POW in VCC.	This approach does not consider security and privacy.
[59]	The system monitors the driver while the vehicle is roaming on the road.	This approach does not address security and privacy.
[60]	The proposed architecture outperforms the architecture proposed in [17].	This study does not provide any security or privacy solutions.
[61]	The study uses a new hierarchical architecture for VCC.	This approach does not address security and privacy.
[63]	The authors use a cyber physical system with a VC.	This study mentions security issues but does not provide any solutions.
[64]	The system protects location confidentiality from external intruders.	This study does not show how the vehicle communicates with the cloud if there are no RSUs on the road.
[66]	The system authenticates the pseudonyms of vehicles while the vehicle is roaming on the road.	RSUs do not have prior information about vehicles; therefore, a legitimate vehicle can be attacked by a malicious vehicle.
[67]	The vehicle's key changes every roaming among RSUs.	This approach causes overhead on the vehicle's OBU.
[68]	The proposed scheme outperforms the scheme proposed in [67] and has a lightweight key management protocol.	The intruder can easily intercept and modify packets that transmit between RSUs and the traffic authority department in the central cloud.
[69]	The system provides two services: accident management services and payment services.	The vehicle cannot communicate with the central cloud if the vehicle is outside the range of the RSU.
[71]	The system prevents Sybil and tracking attacks.	An intruder can intercept and modify the vehicle details when the data are passing between the RSUs' cloudlets.
[93]	The system uses two new services in VCC.	This study does not consider security and privacy issues.
[94]	The system integrates VANET with cloud computing.	This study does not mention communication between vehicles and RSUs and does not consider security and privacy issues.
[96]	The DMV sends pseudonyms to the tamper-resistant hardware in both the OBU and RA.	This approach increases overhead communication on the OBU.
[98]	The study proposes a novel video reporting architecture in a 5G-enabled vehicular network.	The study does not show where the CRL is stored in the vehicle or TA.
[99]	Compared to the approach proposed in [98], this approach reduces the communication cost by 50%.	The communication overhead is increased for the DMV.
[100]	This study addresses some security issues found in [99].	The integrity of video data is not considered in the different layers.
[101]	A participating vehicle uses one pseudonymous certificate for each critical event.	The channels between participating vehicles and the cloud platform are insecure.

Wang *et al.* [110] published the results of a comprehensive survey on the privacy and security of 6G networks. The authors discussed four main aspects: AI-based edge computing, real-time intelligent fog computing, 3D interfaces, and intelligent radio. The authors showed that 6G technology is faster than 5G and offers space-ground-undersea (SGU) coverage. The authors also outlined security and privacy issues for autonomous driving, blockchains, multisensory applications, and wireless brain–computer interactions. These concerns include authentication, access control, encryption, malicious behavior, and communication. Moreover, real-time intelligent edge computing (e.g., in the case of UAV and autonomous vehicle applications) cannot be implemented in 5G because such computing requires ultra-low latency networks, which can be achieved only with 6G technology. In addition, the authors outlined the challenges in deploying 6G in AI applications, physical layers, and network layers. Although the authors' study provided valuable

TABLE 2. A comparison table of security techniques based on video data service in VCC.

Techniques	[96]	[98]	[99]	[101]	[102]
Pseudonymous Certificates		✓	✓	✓	✓
Public Key with Keyword Search		✓	✓	✓	✓
Ciphertext-Policy Attribute-Based Encryption		✓		✓	
Hash Function	✓				
Elliptic Curve Cryptography	✓	✓	✓	✓	✓
Attribute-Based Encryption			✓		✓
Anonymous Credential			✓		
Certificate Signature		✓	✓	✓	
Hash Message Authentication Code (HMAC)					✓
ElGamal Encryption	✓				
Threshold Schemes Based on Secret Sharing		✓			

information about the security and privacy challenges entailed in 6G network usage, the study failed to provide solutions to these issues.

Tang *et al.* [111] proposed a heterogeneous architecture by integrating machine learning (ML) approaches in vehicular networks using 6G. The authors offered an overview of the VANET, Internet of Vehicles (IoVs), UAVs, and air-to-ground (AG) communication. Moreover, this study outlined the main challenges in vehicular applications; these challenges include radio configuration, multi-radio access, beamforming, network allocation, network traffic control, high mobility, privacy requirements, and real-time application requirements. Real-time requirements are highly sensitive in vehicular networks, which require immediate decision-making regarding specific events in real time and attack detection mechanisms. However, security and privacy solutions have not been discussed yet.

The two upcoming networks, 5G and 6G, will change the communication methods among devices, especially for self-driving. Table 3 shows the comparison between 5G and 6G based on several important features, such as mobility, latency, data rate, seif-driving, real-time services, AI integration, VCC, reliability, maximum bandwidth, and key technologies.

According to the above literature, some of studies focus on video recording, taking pictures of critical events in passive mode, and then uploading the pictures to the central cloud computing; see Table 1. These videos and pictures have sensitive information and should be protected against intruders. However, these approaches suffer from both of high latency because of the long distance from the vehicle to the central cloud and an increasing overhead on traffic authorities because the vehicles can send the same video or picture more than once.

Security and privacy are the main concerns of real-time service in VCC. Table 2 shows the security and privacy techniques that are used to secure video data service when data are transmitted among vehicles and infrastructures. These techniques are vulnerable to quantum attack [112]. To apply real-time video surveillance service in a VCC environment, certain requirements should be achieved when designing a robust system architecture model; these requirements include low latency, mobility, scalability, security, and privacy. Moreover, a design for an architecture for real-time video surveillance service should support four factors: real-time data collection, real-time processing, real-time decision-making, and real-time notification messages. Therefore, we can argue that real-time video surveillance data service will play an important role in ITS for monitoring the critical event in the rural and modern cities.

IV. DISCUSSION AND OPEN ISSUES

This section will discuss the importance of real-time video surveillance data in two sections. The first section discusses the usefulness of using real-time video surveillance data in VCC, while the second section is a literature discussion. Finally, the open issues of real-time video surveillance data in VCC are discussed.

A. DISCUSSION OF THE USEFULNESS OF USING REAL-TIME VIDEO SURVEILLANCE DATA IN VCC

The authors believe that real-time video surveillance data service will play a prominent and vital role in the development

and improvement of ITSs in the near future. This service aims to monitor the critical and normal events in both rural and metropolitan cities by monitoring vehicles and pedestrians by capturing a real-time video of the event and sending the video to the traffic authority for processing and decision-making in real-time.

Moreover, unlike traditional vehicular networks (VANETs), VCC systems provide a suitable environment to implement real-time video surveillance data. In VCC, the group of autonomous vehicles (AVs) can share, communicate process, compute, and exchange real-time video surveillance data in the dynamic and static mode of VCC. By using AI systems, the AVs should be able to record any abnormal event that is faced on the road. In addition, the integration between AVs and real-time video surveillance data in VCC will bring advantages in ITS environments and security and privacy challenges and issues. One of the advantages of integration in VCC is that VCC can give a clear picture for traffic authorities to enhance and improve the traffic flow on the road and to make decisions about events according to traffic authority in the real world. This scenario will reduce both communication overhead and latency on traffic authority by making the processing and decision-making of real-time video data in the edge of the network. For instance, the VCC and surveillance services will automate minor accident procedures by photographing vehicular accidents and signing documents electronically by using the identity of the AV or the identity of the driver (if the vehicle is not fully autonomous) without needing the presence of a police officer or the insurance company.

One of the most prominent obstacles that real-time video monitoring systems in VCC will face is that the current road infrastructure is unsuitable for this type of real-time service, so the road infrastructure should be developed with the latest network technologies, such as 5G networks and future 6G networks, which fully support AVs. Undoubtedly, these developments and improvements require high revenues from transport institutions and authorities to create a powerful road infrastructure that keeps pace with the rapid technological changes in the world and supports self-driving vehicles (or autonomous vehicles). Self-driving vehicles need to be continuously connected to the internet, so any interruption in communication will lead to traffic disasters and many casualties, so designing a communication method is very important to ensure the smooth movement of self-driving vehicles to record real-time video data on the roads.

The authors in [114] presented a technical note for ongoing research on connected vehicles. This technical note starts by discussing roadway infrastructure classification which consist of four classes. The authors show the importance of improving the road infrastructure to support automation vehicles. Then, the authors discuss the main challenges and the importance of appropriate infrastructure provisions to support CAV operations. Although this study gives important information on the importance of enhancing and developing road infrastructure, this study does not mention real-time services in VCC. Similarly, in [115], the authors show the importance of broadband technology in enhancing the transportation system. Broadband technology is highly important for achieving communication between vehicles and humans. Moreover, the engineers need to develop a powerful transportation system and road infrastructure to support real-time services and applications.

Tariq in [116] proposed a real option analysis (ROA) framework to overcome the limitations in road infrastructure. One of the main objectives of this dissertation is to propose transportation agency guidelines in the context of AVs. Moreover, the researcher gave important recommendations regarding the importance of road infrastructure and the cooperation of self-driving car manufacturers before starting to actually operate AVs on the roads to avoid any potential human or environmental disasters. Therefore, there is an urgent need to build a robust and efficient model for implementing real-time video surveillance services, especially in areas that lack infrastructure.

In [117], the authors explore the preferences of prospective future AVs consumers according to four choices of AVs. These four choices of AVs are self-owned AVs, private AVs, vehicle-sharing AVs and ride-hailing AVs. This study aims to determine the trend and measure the relative impact of different characteristics related to travel behavior and awareness of the importance of technology in autonomous vehicles among people. Moreover, this study reviewed AV patterns that can be developed and become a reality in the future by taking the opinions of the public and vehicle drivers on the development of road infrastructure. The findings show that consumers prefer to use traditional vehicles rather than AVs because consumers are unaware of the importance of self-driving vehicles in reducing accidents and complying with traffic safety laws. Therefore, the authors completely agree with the recommendation and vision in [114]–[117] because the recommendation will enhance the quality of safety and traffic flow on the road and protect the life of drivers and passengers.

In terms of security and privacy, protecting real-time video surveillance data, modern vehicles, and AVs are mandatory because most modern cars and AVs are connected to the internet, thus making them vulnerable to adversaries who can manipulate, alter, insert, or generate fake real-time video surveillance data during data transmission through the network. Therefore, the security and privacy requirements should be achieved when designing a system model for real-time service in VCC by designing effective security and privacy algorithms to protect both real-time video surveillance data, modern vehicles and AVs on the road.

B. DISCUSSION LITERATURE

In this review, we cover different video data and POW services in VCCs. The authors proposed a POW service that enables a vehicle's camera to record videos and take a picture in the passive mode. These videos and pictures were uploaded to traffic authorities in remote clouds by using DSRC and

TABLE 3. A comparison table between 5G and 6G.

Features	5G	6G
Mobility	Up to 500 Km/h	Up to 1000 Km/h
Latency	10 ms	Close to zero
Data Rate	10 Gbps	1 Tbsp.
Self-driving	Partial	Fully
Real-Time Services	Partial	Fully
AI Integration	Patrial	Fully
Vehicular Cloud Support	Partial	Fully
Reliability	99.999 %	Approximately 99.9 %
Maximum Bandwidth	1 GHz	100 GHz
Key Technologies	D2D communication, mmWave, small cells, Massive Multi-input multi-output (mMIMO) [113].	Visible Light Communication (VLC).

4G communication. These two types of communication suffer from scalability, mobility, and latency because of the long distance between the vehicles and the central cloud. These approaches aim to monitor the driver and events on the road. Moreover, there is no benefit to just recording video or taking pictures without taking a decision except work in [94]. The authors mentioned that the video recordings and pictures are processed by the traffic authority for decision-making; then, the police vehicle is notified to attend the events location. However, the security and privacy issues have not yet been fully addressed.

The approaches in [98]–[102] proposed a new surveillance service called video reporting for monitoring drivers and events in vehicular network environments. In the proposed methods, vehicles record abnormal events on the road and send the associated data to traffic authorities in the central cloud, after which an official vehicle accesses the cloud to explore the video. These video recording data are uploaded using D2D communication and mmWave technology, which are used in 5G networks to overcome the limitations of DSRC and 4G. Compared to previous studies, the authors improved the scalability and latency, but the latency is still high because of the long distance between vehicles and the central cloud. Moreover, the authors did not show how the official vehicles knew there was an event to access the cloud, download the video, and then go to the event's location.

This scenario may affect traffic flow and the lives of drivers, passengers and pedestrians. As a result, existing approaches are based on centralized traffic authorities to generate security policies that lead to security issues. Maintaining security policies in centralized traffic authorities has weaknesses, such as a single point of failure. Moreover, availability is one of the main requirements of real-time video services to make participating and official vehicles upload real-time critical event video data anywhere and anytime.

Fortunately, the authors did not consider the importance of using video reporting data in real time. The approaches of the authors are unacceptable for real-time video reporting and surveillance data services, owing to the time sensitivity of the process of recording events and sending the recordings to the traffic authority for decision-making. To design a new architecture for real-time services in VCC, ultralow latency, mobility, location-awareness scalability, availability, security, and privacy requirements should be considered.

Finally, researchers expect 5G technology to be fully deployed by the beginning of 2023. However, this technology can partially support real-time video surveillance data services and applications, especially those concerning AVs, which require quick decision-making and processing of events (such as accidents) in real time with ultra-low latency.

The 5G and 6G technologies will become mandatory for all intelligent networks in the future because both 5G and 6G technologies will cause a major revolution in VCC, as modern vehicles and AVs will not only exchange or store information but also process the data and make decisions in real time without relying on CC. Moreover, the integration of 5G and 6G will bring new significant security and privacy challenges for real-time services in VCCs. Therefore, the most open issues in the security and privacy of real-time video surveillance data in VCC are as follows.

- Real-Time High-Mobility Authentication: Authentication is an important security requirement in VCC, especially for high-mobility authentication. In VCC, the modern vehicle, AV, RSU, and the central cloud should be authenticated before sending any safety or non-safety messages among its and other entities. Vehicles on the road can be static, semi-dynamic, or highly dynamic. First, a static vehicle is a vehicle in static mode, such as when the vehicle is parked at a shopping mall for a long time. Second, a semi-dynamic vehicle is a vehicle that moves at 40 km/h in the city. Third, a highly dynamic vehicle is a vehicle that moves at a very high speed (such as 150 km/h) inside a city or highway. High-dynamic

TABLE 4. A comparison table of video data and POW services in VCC. ✓: Fully achieved, * partially achieved, ✗: Not achieved.

Ref.	Security	Data Privacy	Identity Privacy	Vehicular Network	Communication Type	Latency	Scalability	High Mobility
[17]	✗	✗	✗	VuC	DSRC	High	✗	✗
[58]	✗	✗	✗	VuC	DSRC	High	✗	✗
[59]	✗	✗	✗	VuC	DSRC	High	✗	✗
[61]	✓	*	*	VANET	DSRC	High	✗	✗
[63]	✗	✗	✗	VuC	DSRC	High	✗	✗
[64]	✗	✗	✗	VuC	DSRC	High	✗	✗
[65]	*	✗	*	VuC	DSRC	High	✗	✗
[66]	✗	✗	✗	VuC	DSRC	High	✗	✗
[68]	✓	*	✓	VuC	DSRC/4G	High	*	✗
[84]	*	✗	✗	VANET	DSRC	High	✗	✗
[85]	✗	✗	✓	VANET	DSRC	High	✗	✗
[86]	✗	✗	✗	VuC	DSRC	High	✗	✗
[87]	✗	✗	✗	VuC	DSRC	High	✗	✗
[91]	✓	✓	✓	VuC	DSRC /4G	High	✓	✗
[93]	✓	✓	✓	VuC	D2D	Moderated	✓	✗
[94]	✓	✓	✓	VuC	5G	Low	✓	✗
[95]	✗	*	✗	VC	Not mentioned	Not mentioned	✗	✗
[96]	✓	*	✓	VuC	D2D	Moderated	✓	✗
[97]	✓	✓	✓	VuC	5G	Moderated	*	✗

vehicle authentication is a challenge faced by VCCs because the vehicle roams between different locations in a few seconds and the vehicle's identity needs to be authenticated in every movement. Thus, a novel mechanism is required to authenticate the high mobility of vehicles in VCCs.

- Real-Time Video Data Integrity: Integrity is one of the security requirements responsible for protecting the data from any new information that may be added by intruders during transmission on the network. For instance, the vehicle records a video of an event from the road and sends two messages. The first message consists of an event video as a plain message, while the second message is a hashed event video by using a hashing algorithm in the RSUs or traffic authority. The receiver should compare the two messages received from the sender by hashing the plain message and comparing the message with the original event video hash. Using a robust key in the hashing algorithm is required; however, the computation of the key should not take a long time to hash the event data.
- Real-time Video Data Confidentiality: Vehicles or RSUs can record and exchange sensitive data regarding any event (such as accidents or traffic jams) with other vehicles on the road. These events contain either normal or sensitive data. More clearly, normal data do not need decision-making from the traffic authority, whereas sensitive data require urgent decision-making from the traffic authority in real time. In addition, the sensitive data sent by the vehicle or RSU to traffic authorities should be protected from internal and external attackers using symmetric or asymmetric algorithms. Lightweight cryptography is required to avoid computation overhead on the OBU or RSU.
- Real-Time Vehicle Location: Securing the real-time vehicle location is another challenge in the VCC environment. The vehicle sends the location for each event, either a normal event or urgent event, to the traffic authority; this information is combined with the vehicle's identity, vehicle's location, type of event, time of recording (if the event is recorded by the vehicle's camera), and the traffic authority identity. For sensitive events that require decision-making, a notification that the message was received should be sent by the traffic authority to the current vehicle location. However, a new technique is required to protect the location of vehicles from intruders.

Finally, Table 4 compares the approaches that used video data and POW services in VCC. The approaches were compared based on security, data privacy, identity privacy, vehicular network types, communication type, latency, scalability, and high mobility requirements. However, these requirements are important for delivering real-time video data from vehicles and infrastructure in VCCs.

V. CONCLUSION

VCC will play an important role in ITS in the near future. Moreover, real-time video surveillance will change the

concept of surveillance service on the road by allowing for a clear picture of traffic flow on the roads and assisting the traffic authorities for improving and enhancing traffic safety in rural areas and modern cities. AVs consist of intelligent sensors that enable vehicles to collect real-time video surveillance data from inside and outside vehicle. These real-time video surveillance data include sensitive data that should be protected against intruders when the data are transmitted through the network. Nevertheless, to apply real-time surveillance services in VCC, certain requirements should be fulfilled when designing the system model; these requirements include ultra-low latency, scalability, availability, high-mobility, security and privacy. Therefore, the security and privacy solutions for real-time video reporting and surveillance data have not yet been fully addressed in the VCC environment.

After reviewing several studies, this study conducted a survey to secure and protect video data services in VCCs from internal and external intruders. A taxonomy for securing real-time data video services is presented by adding new classifications that have not been considered in the literature. A comparison table was added to the relevant studies that focused on video data services. Then, this survey pointed out the importance of 5G and 6G in real-time video data services in VCC. Finally, the challenges and open issues of real-time video surveillance data are presented.

In our opinion, the future research direction for real-time video surveillance data in VCC should be focused on security and privacy issues, such as protecting vehicle identity, vehicle location identity, event location, real-time data integrity, real-time data confidentiality, and privacy preserving because the real-time video data can be manipulated, altered and sniffed by intruders when transmitted among entities in VCC. The intruders can generate fake real-time video surveillance data and send them to vehicles as trusted data. To tackle these challenges, more research studies are needed to improve and enhance the security and privacy of real-time video data in VCC. However, the current security and privacy techniques are unsuitable for securing and protecting real-time video surveillance data in VCC. Therefore, a robust and efficient security protocol is required to handle all types of security and privacy threats.

Finally, in VCC, vehicles not only send real-time video surveillance data but also share their identities, current location, speed, time, and direction. These factors should be protected from intruders to provide reliability and privacy when real-time video data are transmitted among vehicles and infrastructures. As a result, new sophisticated and robust cryptography algorithms are needed to provide powerful security and privacy for real-time video surveillance data when transmitted among V2V and V2I communications.

ACKNOWLEDGMENT

The authors would like to thank the Scientific Research Deanship's for technical and financial support.

REFERENCES

[1] A. Dimovski. *Car Accident Statistics in the U.S.A-2020 Infographic*. CARSURANCE. Accessed: Nov. 4, 2021. [Online]. Available: https://carsurance.net/blog/car-accident-statistics/

[2] S. Yousefi, M. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): Challenges and perspectives," in *Proc. 6th Int. Conf. ITS Telecommun.*, Chengdu, China, Jun. 2006, pp. 761–766.

[3] H. Jiang, S. Chen, Y. Yang, Z. Jie, H. Leung, J. Xu, and L. Wang, "Estimation of packet loss rate at wireless link of VANET-RPLE," in *Proc. Int. Conf. Comput. Intell. Softw. Eng.*, Chengdu, China, Sep. 2010, pp. 1–5.

[4] R. Kumar and M. Dave, "A comparative study of various routing protocols in VANET," 2011, *arXiv:1108.2094*.

[5] D. S. Gaikwad and M. Zaveri, "VANET routing protocols and mobility models: A survey," in *Trends in Network and Communications*. Springer: Berlin, Germany, 2011, pp. 334–342.

[6] M. Sood and S. Kanwar, "Clustering in MANET and VANET: A survey," in *Proc. Int. Conf. Circuits, Syst., Commun. Inf. Technol. Appl. (CSCITA)*, Mumbai, India, Apr. 2014, pp. 375–380.

[7] K.-C. Lan and C.-M. Chou, "Realistic mobility models for vehicular ad hoc network (VANET) simulations," in *Proc. 8th Int. Conf. ITS Telecommun.*, Phuket, Thailand, Oct. 2008, pp. 362–366.

[8] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network—Performance evaluation," *Transp. Res. C, Emerg. Technol.*, vol. 68, pp. 168–184, Jul. 2016, doi: 10.1016/j.trc.2016.03.008.

[9] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.

[10] M. I. Hassan, H. L. Vu, and T. Sakurai, "Performance analysis of the IEEE 802.11 MAC protocol for DSRC safety applications," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3882–3896, Jul. 2011, doi: 10.1109/TVT.2011.2162755.

[11] C. So-In, R. Jain, and A.-K. Tamimi, "Scheduling in IEEE 802.16e mobile WiMAX networks: Key issues and a survey," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 2, pp. 156–171, Feb. 2009, doi: 10.1109/JSAC.2009.090207.

[12] Z. Xu, X. Li, X. Zhao, M. H. Zhang, and Z. Wang, "DSRC versus 4G-LTE for connected vehicle applications: A study on field experiments of vehicular communication performance," *J. Adv. Transp.*, vol. 2017, Aug. 2017, Art. no. 2750452, doi: 10.1155/2017/2750452.

[13] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018, doi: 10.1109/ACCESS.2017.2779844.

[14] S. Olariu, I. Khalil, and M. Abuelela, "Taking VANET to the clouds," *Int. J. Pervasive Comput. Commun.*, vol. 7, no. 1, pp. 7–21, May 2011, doi: 10.1108/17427371111123577.

[15] 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 *Proc. 5th Int. Conf. Syst. Netw. Commun.*, Nice, France, Aug. 2010, pp. 117–123.

[16] H. Rasheed, R. Zeinab, and O. Heekuck, "A paradigm shift from vehicular ad hoc networks to VANET-based clouds," *Wireless Pers. Commun.*, vol. 83, no. 2, pp. 1131–1158, Feb. 2015, doi: 10.1007/s11277-015-2442-y.

[17] M. Gerla, J.-T. Weng, and G. Pau, "Pics-on-wheels: Photo surveillance in the vehicular cloud," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, San Diego, CA, USA, Jan. 2013, pp. 1123–1127.

[18] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Sep. 2013, doi: 10.1109/TITS.2012.2211870.

[19] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds," in *Proc. 6th Int. Conf. Complex, Intell., Softw. Intensive Syst.*, Palermo, Italy, Jul. 2012, pp. 370–375.

[20] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A survey on vehicular cloud computing," *J. Netw. Comput. Appl.*, vol. 40, pp. 325–344, Mar. 2014, doi: 10.1016/j.jnca.2013.08.004.

[21] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, Jan. 2021, doi: 10.1007/s11235-020-00733-2.

[22] R. Sheikh, M. S. Chande, and D. K. Mishra, "Security issues in MANET: A review," in *Proc. 7th Int. Conf. Wireless Opt. Commun. Netw. (WOCN)*, Colombo, Sri Lanka, Sep. 2010, pp. 1–4.

[23] A. Nadeem and M. P. Howarth, "A survey of MANET intrusion detection prevention approaches for network layer attacks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 2027–2045, Mar. 2013, doi: 10.1109/SURV.2013.030713.00201.

[24] D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa, and R. H. Jhaveri, "A survey of reactive routing protocols in MANET," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Chennai, India, Feb. 2014, pp. 1–6.

[25] J. Mittag, F. Thomas, J. Härri, and H. Hartenstein, "A comparison of single- and multi-hop beaconing in VANETs," in *Proc. 6th ACM Int. workshop Veh. InterNETworking (VANET)*, Beijing, China, 2009, pp. 69–78.

[26] S. Usha and S. Radha, "Co-operative approach to detect misbehaving nodes in MANET using multi-hop acknowledgement scheme," in *Proc. Int. Conf. Adv. Comput., Control, Telecommun. Technol.*, Bengaluru, India, Dec. 2009, pp. 576–578.

[27] F. Bai, D. D. Stancil, and H. Krishnan, "Toward understanding characteristics of dedicated short range communications (DSRC) from a perspective of vehicular network engineers," in *Proc. 16th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, Chicago, IL, USA, 2010, pp. 329–340.

[28] N. Ganeshkumar and S. Kumar, "OBU (on-board unit) wireless devices in VANET(s) for effective communication—A review," in *Computational Methods and Data Engineering*. Singapore: Springer, 2021, pp. 191–202.

[29] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," *Int. J. Netw. Secur. Appl.*, vol. 5, no. 5, pp. 95–105, Sep. 2013, doi: 10.5121/ijnsa.2013.5508.

[30] Y.-N. Liu, S.-Z. Lv, M. Xie, Z.-B. Chen, and P. Wang, "Dynamic anonymous identity authentication (DAIA) scheme for VANET," *Int. J. Commun. Syst.*, vol. 32, no. 5, p. e3892, Mar. 2019, doi: 10.1002/dac.3892.

[31] T. Mastelic, A. Oleksiak, H. Claussen, I. Brandic, J.-M. Pierson, and A. V. Vasilakos, "Cloud computing: Survey on energy efficiency," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–36, Jan. 2015, doi: 10.1145/2656204.

[32] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Mar. 2017, doi: 10.1016/j.jnca.2017.02.001.

[33] B. Furht, "Cloud computing fundamentals," in *Handbook of Cloud Computing*, B. Furht and A. Escalante, Eds. Boston, MA, USA: Springer, 2010, pp. 3–19.

[34] D. Freet, R. Agrawal, S. John, and J. J. Walker, "Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS," in *Proc. 7th Int. Conf. Manage. Comput. Collective Intell. Digit. EcoSyst.*, Caraguatatuba, Brazil, Oct. 2015, pp. 148–155.

[35] M. Gerla, "Vehicular cloud computing," in *Proc. 11th Ann. Medit. Ad Hoc Netw. Workshop (Med-Hoc-Net)*, New York, NY, USA, 2012, pp. 152–155.

[36] E. Lee, E.-K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: Architecture and design principles," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 148–155, Feb. 2014, doi: 10.1109/MCOM.2014.6736756.

[37] K. Zheng, H. Meng, P. Chatzimisios, L. Lei, and X. Shen, "An SMDP-based resource allocation in vehicular cloud computing systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 12, pp. 7920–7928, Sep. 2015, doi: 10.1109/TIE.2015.2482119.

[38] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2725–2764, Jul. 2020, doi: 10.1109/COMST.2020.3012961.

[39] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012, doi: 10.1007/s11235-010-9400-5.

[40] Y. Wei and M. B. Blake, "Service-oriented computing and cloud computing: Challenges and opportunities," *IEEE Internet Comput.*, vol. 14, no. 6, pp. 72–75, Nov. 2010, doi: 10.1109/MIC.2010.147.

[41] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, "A survey on green 6G network: Architecture and technologies," *IEEE Access*, vol. 7, pp. 175758–175768, 2019, doi: 10.1109/ACCESS.2019.2957648.

[42] J. Janech, A. Lieskovsky, and E. Krsak, "Comparation of strategies for data replication in VANET environment," in *Proc. 26th Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Fukuoka, Japan, Mar. 2012, pp. 575–580.

[43] M. Eberhard and M. Tarpenning, *The 21st Century Electric Car Tesla Motors*. San Carlos, CA, USA: Tesla Motors, 2006.

[44] *Luxury Electric Cars*. Accessed: Nov. 7, 2021. [Online]. Available: https://www.lucidmotors.com

[45] B. Fleming, "Advances in automotive electronics [automotive electronics]," *IEEE Veh. Technol. Mag.*, vol. 10, no. 4, pp. 4–96, Dec. 2015, doi: 10.1109/MVT.2015.2481008.

[46] R. Ramnath, N. Kinnear, S. Chowdhury, and T. Hyatt, "Interacting with Android auto and apple CarPlay when driving: The effect on driver performance," IAM RoadSmart, Wokingham, U.K., Project Rep. PPR948, 2020.

[47] J. Qin, H. Zhu, Y. Zhu, L. Lu, G. Xue, and M. Li, "POST: Exploiting dynamic sociality for mobile advertising in vehicular networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 6, pp. 1770–1782, Aug. 2016, doi: 10.1109/TPDS.2015.2467392.

[48] F. Dötzer, "Privacy issues in vehicular Ad Hoc networks," in *Privacy Enhancing Technologies*, G. Danezis and D. Martin, Eds. Berlin, Germany: Springer, 2006, pp. 197–209.

[49] T. Leinmuller, E. Schoch, and C. Maihofer, "Security requirements and solution concepts in vehicular ad hoc networks," in *Proc. 4th Annu. Conf. Wireless Demand Netw. Syst. Services*, Obergurgl, Austria, Jan. 2007, pp. 84–91.

[50] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart. Sep. 2008, doi: 10.1109/COMST.2008.4625806.

[51] D. A. Rivas, J. M. Barceló-Ordinas, M. G. Zapata, and J. D. Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information and secure data aggregation," *J. Netw. Comput. Appl.*, vol. 34, no. 6, pp. 1942–1955, Nov. 2011, doi: 10.1016/j.jnca.2011.07.006.

[52] S. khan, I. Sharma, M. Aslam, M. Z. Khan, and S. Khan, "Security challenges of location privacy in VANETs and state-of-the-art solutions: A survey," *Future Internet*, vol. 13, no. 4, pp. 1–22, Apr. 2021, doi: 10.3390/fi13040096.

[53] J. Grover, "Security of vehicular ad hoc networks using blockchain: A comprehensive review," *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100458, doi: 10.1016/j.vehcom.2022.100458.

[54] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007, doi: 10.3233/JCS-2007-15103.

[55] P. Papadimitratos, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008, doi: 10.1109/MCOM.2008.4689252.

[56] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 8–15, Nov. 2006, doi: 10.1109/WC-M.2006.250352.

[57] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Nov. 2006, doi: 10.1109/WC-M.2006.250353.

[58] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for vanet," in *Proc. 5th ACM Int. Workshop Veh. InterNETworking (VANET)*, San Francisco, CA, USA, 2008, pp. 88–89.

[59] M. Abuelela and S. Olariu, "Taking VANET to the clouds," in *Proc. 8th Int. Conf. Adv. Mobile Comput. Multimedia (MoMM)*, Paris, France, 2010, pp. 6–13.

[60] F. Ahmad, M. Kazim, A. Adnane, and A. Awad, "Vehicular cloud networks: Architecture, applications and security issues," in *Proc. IEEE/ACM 8th Int. Conf. Utility Cloud Comput. (UCC)*, Limassol, Cyprus, Dec. 2015, pp. 571–576.

[61] M. Garai, S. Rekhis, and N. Boudriga, "Communication as a service for cloud VANETs," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Larnaca, Cyprus, Jul. 2015, pp. 371–377.

[62] J. Wan, D. Zhang, Y. Sun, K. Lin, C. Zou, and H. Cai, "VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing," *Mobile Netw. Appl.*, vol. 19, no. 2, pp. 153–160, Apr. 2014, doi: 10.1007/s11036-014-0499-6.

[63] J. Wan, D. Zhang, S. Zhao, L. T. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 106–113, Aug. 2014, doi: 10.1109/MCOM.2014.6871677.

[64] G. Yan, S. Olariu, and M. C. Weigle, "Providing location security in vehicular Ad Hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55, Dec. 2009, doi: 10.1109/MWC.2009.5361178.

[65] K. Mershad and H. Artail, "Finding a STAR in a vehicular cloud," *IEEE Intell. Transp. Syst. Mag.*, vol. 5, no. 2, pp. 55–68, Apr. 2013, doi: 10.1109/MITS.2013.2240041.
[66] Y. Park, C. Sur, and K.-H. Rhee, "Pseudonymous authentication for secure V2I services in cloud-based vehicular networks," *J. Ambient Intell. Hum. Comput.*, vol. 7, no. 5, pp. 661–671, Jul. 2015, doi: 10.1007/s12652-015-0309-4.
[67] R. Hussain, Z. Rezaeifar, Y.-H. Lee, and H. Oh, "Secure and privacy-aware traffic information as a service in VANET-based clouds," *Pervas. Mobile Comput.*, vol. 24, pp. 194–209, Dec. 2015, doi: 10.1016/j.pmcj.2015.07.007.
[68] L. Nkenyereye and K. H. Rhee, "Secure traffic data transmission protocol for vehicular cloud," in *Advances in Computer Science and Ubiquitous Computing*, D.-S. Park, H.-C. Chao, Y.-S. Jeong, and J. J. Park, Eds. Singapore: Springer, 2015, pp. 497–503.
[69] W. Kang, J. Lee, Y.-S. Jeong, and J. Park, "VCC-SSF: Service-oriented security framework for vehicular cloud computing," *Sustainability*, vol. 7, no. 2, pp. 2028–2044, Feb. 2015, doi: 10.3390/su7022028.
[70] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PLoS ONE*, vol. 15, no. 2, Feb. 2020, Art. no. e0228319, doi: 10.1371/journal.pone.0228319.
[71] M. Garai, S. Rekhis, and N. Boudriga, "A vehicular cloud for secure and QoS aware service provision," in *Advances in Ubiquitous Networking*, vol. 2, R. El-Azouzi, D. S. Menasche, E. Sabir, F. De Pellegrini, and M. Benjillali, Eds. Singapore: Springer, 2017, pp. 219–233.
[72] M. A. Saleem, S. Zhou, A. Sharif, T. Saba, M. A. Zia, A. Javed, S. Roy, and M. Mittal, "Expansion of cluster head stability using fuzzy in cognitive radio CR-VANET," *IEEE Access*, vol. 7, pp. 173185–173195, 2019, doi: 10.1109/ACCESS.2019.2956478.
[73] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *Cogn. Syst. Res.*, vol. 55, pp. 153–163, Jun. 2019, doi: 10.1016/j.cogsys.2019.01.008.
[74] S. Sharma and A. Kaul, "VANETs cloud: Architecture, applications, challenges, and issues," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 2081–2102, Jun. 2021, doi: 10.1007/s11831-020-09447-9.
[75] Q.-V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, H. Won-Joo, and Z. Ding, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116974–117017, 2020, doi: 10.1109/ACCESS.2020.3001277.
[76] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Jul. 2019, doi: 10.1109/JIOT.2019.2927379.
[77] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018, doi: 10.1109/ACCESS.2017.2779146.
[78] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, May 2019, doi: 10.1109/COMST.2019.2916180.
[79] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5G communications," in *Fundamentals of 5G Mobile Networks*, J. Rodriguez, Ed. Hoboken, NJ, USA: Wiley, 2015, pp. 207–220.
[80] M. Alam, D. Yang, J. Rodriguez, and R. Abd-alhameed, "Secure device-to-device communication in LTE-A," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 66–73, May 2014, doi: 10.1109/MCOM.2014.6807948.
[81] S. T. Shah, S. F. Hasan, B.-C. Seet, P. H. J. Chong, and M. Y. Chung, "Device-to-device communications: A contemporary survey," *Wireless Pers. Commun.*, vol. 98, no. 1, pp. 1247–1284, Jan. 2018, doi: 10.1007/s11277-017-4918-4.
[82] A. P. G. Lopes and P. R. L. Gondim, "Group authentication protocol based on aggregated signatures for D2D communication," *Comput. Netw.*, vol. 178, Sep. 2020, Art. no. 107192, doi: 10.1016/j.comnet.2020.107192.
[83] J. Cao, M. Ma, and H. Li, "Gbaam: Group-based access authentication for MTC in LTE networks," *Security Commun. Netw.*, vol. 8, no. 17, pp. 3282–3299, Nov. 2015, doi: 10.1002/sec.1252.
[84] *3GPP Portal*. Accessed: Nov. 7, 2021. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=810
[85] N. Li, "Research on Diffie–Hellman key exchange protocol," in *Proc. 2nd Int. Conf. Comput. Eng. Technol.*, Chengdu, China, 2010, p. 634.
[86] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Cryptographic Hardware and Embedded Systems*, vol. 2001, Ç. K. Koç, D. Naccache, and C. Paar, Eds., Berlin, Germany: Springer, 2001, pp. 309–318.
[87] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Comput. Commun.*, vol. 32, no. 6, pp. 1079–1085, Apr. 2009, doi: 10.1016/j.comcom.2008.12.042.
[88] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000, doi: 10.1023/A:1008354106356.
[89] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, "Mobeyes: Smart mobs for urban monitoring with a vehicular sensor network," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 52–57, Nov. 2006, doi: 10.1109/WC-M.2006.250358.
[90] P. Bellavista, E. Magistretti, U. Lee, and M. Gerla, "Standard integration of sensing and opportunistic diffusion for urban monitoring in vehicular sensor networks: The MobEyes architecture," in *Proc. IEEE Int. Symp. Ind. Electron.*, Vigo, Spain, Jun. 2007, pp. 2582–2588.
[91] M. Kutila, P. Pyykönen, A. Lybeck, P. Niemi, and E. Nordin, "Towards autonomous vehicles with advanced sensor solutions," *World J. Eng. Technol.*, vol. 3, no. 3, pp. 6–17, 2015, doi: 10.4236/wjet.2015.33C002.
[92] N. Kose, O. Kopuklu, A. Unnervik, and G. Rigoll, "Real-time driver state monitoring using a CNN based spatio-temporal approach," in *Proc. IEEE Intell. Transp. Syst. Conf. (ITSC)*, Auckland, New Zealand, Oct. 2019, pp. 3236–3242.
[93] J. T. Weng, "On demand surveillance service in vehicular cloud," Ph.D. dissertation, Dept. Comput. Sci., UCLA, Los Angeles, CA, USA, 2013.
[94] A. B. Habtie, "Cellular-cloud integration framework in support of real-time monitoring and management of traffic on the road: The case of Ethiopia," in *Proc. Int. Conf. Manage. Emergent Digit. EcoSystems (MEDES)*, Addis Ababa, Ethiopia, 2012, pp. 189–196.
[95] M. Soyturk, K. N. Muhammad, M. N. Avcil, B. Kantarci, and J. Matthews, "Chapter 8—From vehicular networks to vehicular clouds in smart cities," in *Smart Cities and Homes*, M. S. Obaidat and P. Nicopolitidis, Eds. Boston, MA, USA: Morgan Kaufmann, 2016, pp. 149–171.
[96] R. Hussain, F. Abbas, J. Son, D. Kim, S. Kim, and H. Oh, "Vehicle witnesses as a service: Leveraging vehicles as witnesses on the road in VANET clouds," in *Proc. IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, Bristol, U.K., Dec. 2013, pp. 439–444.
[97] Y. Tsiounis and M. Yung, "On the security of ElGamal based encryption," in *Public Key Cryptography*, H. Imai and Y. Zheng, Eds. Berlin, Germany: Springer, 1998, pp. 117–134.
[98] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Mar. 2016, doi: 10.1109/TVT.2016.2541862.
[99] L. Nkenyereye, J. Kwon, and Y.-H. Choi, "Secure and lightweight cloud-assisted video reporting protocol over 5G-enabled vehicular networks," *Sensors*, vol. 17, no. 10, p. 2191, Sep. 2017, doi: 10.3390/s17102191.
[100] Z. A. Almusaylim, N. Zaman, and L. T. Jung, "Proposing a data privacy aware protocol for roadside accident video reporting service using 5G in vehicular cloud networks environment," in *Proc. 4th Int. Conf. Comput. Inf. Sci. (ICCOINS)*, Kuala Lumpur, Malaysia, Aug. 2018, pp. 1–5.
[101] S. G. Yoo, "5G-VRSec: Secure video reporting service in 5G enabled vehicular networks," *Wireless Commun. Mobile Comput.*, vol. 2017, Jul. 2017, Art. no. 7256307, doi: 10.1155/2017/7256307.
[102] A. Mohseni-Ejiyeh and M. Ashouri-Talouki, "SeVR+: Secure and privacy-aware cloud-assisted video reporting service for 5G vehicular networks," in *Proc. Iranian Conf. Electr. Eng. (ICEE)*, Tehran, Iran, May 2017, pp. 2159–2164.
[103] 6G Flagship. *Discover how 6G Will Change Our Lives* Oulu.fi. Accessed: Nov. 4, 2020. [Online]. Available: https://www.oulu.fi/6gflagship/
[104] A. Yastrebova, R. Kirichek, Y. Koucheryavy, A. Borodin, and A. Koucheryavy, "Future networks 2030: Architecture requirements," in *Proc. 10th Int. Congr. Ultra Modern Telecommun. Control Syst. Workshops (ICUMT)*, Moscow, Russia, Nov. 2018, pp. 1–8.
[105] B. Aazhang, P. Ahokangas, V. Alves, and M. Alouini, "Key drivers and research challenges for 6G ubiquitous wireless intelligence (white paper)," 6G Res. Vis., Univ. Oulu, Oulu, Finland, Tech. Rep., Sep. 2019.
[106] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 42–50, Aug. 2019, doi: 10.1109/MVT.2019.2921162.

[107] L. Zhang, Y.-C. Liang, and D. Niyato, "6G visions: Mobile ultra-broadband, super Internet-of-Things, and artificial intelligence," *China Commun.*, vol. 16, no. 8, pp. 1–14, Aug. 2019, doi: 10.23919/JCC.2019.08.001.
[108] K. Sheth, K. Patel, H. Shah, S. Tanwar, R. Gupta, and N. Kumar, "A taxonomy of AI techniques for 6G communication networks," *Comput. Commun.*, vol. 161, pp. 279–303, Sep. 2020, doi: 10.1016/j.comcom.2020.07.035.
[109] L. Lovén, *EdgeAI: A Vision for Distributed, Edge-Native Artificial Intelligence in Future 6G Networks*. Levi, Finland: 6G Wireless Summit, 2019.
[110] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digit. Commun. Netw.*, vol. 6, no. 3, pp. 281–291, Aug. 2020, doi: 10.1016/j.dcan.2020.07.003.
[111] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6G: Machine-learning approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020, doi: 10.1109/JPROC.2019.2954595.
[112] J. Ahn, H. Y. Kwon, B. Ahn, K. Park, T. Kim, M. K. Lee, J. Kim, and J. Chung, "Toward quantum secured distributed energy resources: Adoption of post-quantum cryptography (PQC) and quantum key distribution (QKD)," *Energies.*, vol. 15, no. 3, pp. 1–20, Jan. 2022, doi: 10.3390/en15030714.
[113] A. Shahmansoori, G. E. Garcia, G. Destino, G. Seco-Granados, and H. Wymeersch, "Position and orientation estimation through millimeter-wave MIMO in 5G systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1822–1835, Dec. 2018, doi: 10.1109/TWC.2017.2785788.
[114] T. U. Saeed, B. N. Alabi, and S. Labi, "Preparing Road infrastructure to accommodate connected and automated vehicles: System-level perspective," *J. Infrastruct. Syst.*, vol. 21, no. 1, pp. 1–3, 2021, doi: 10.1061/(ASCE)IS.1943-555X.0000593.
[115] S. Caldwell, C. Hendrickson, and L. R. Rilett, "It is time to recognize communications as a mode of transportation," *J. Transp. Eng.*, vol. 147, no. 7, Jul. 2021, Art. no. 01821002, doi: 10.1061/JTEPBS.0000540.
[116] T. U. Saeed, "Road infrastructure readiness for autonomous vehicles," Ph.D. dissertation, Lyles School Civil Eng., Purdue Univ. Graduate School, West Lafayette, Indiana, Aug. 2019.
[117] T. U. Saeed, M. W. Burris, S. Labi, and K. C. Sinha, "An empirical discourse on forecasting the use of autonomous vehicles using consumers' preferences," *Technol. Forecasting Social Change.*, vol. 158, Sep. 2020, Art. no. 120130, doi: 10.1016/j.techfore.2020.120130.

MAJED S. ALSAYFI received the B.Sc. degree in computer science from Taibah University, Medina, Saudi Arabia, in 2005, and the M.Sc. degree in network security from the University of Sains Malaysia (USM), Penang, Malaysia, in 2010. He is currently pursuing the Ph.D. degree with the Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, Jeddah, Saudi Arabia. His research interests include computer security, information security, network security, security and privacy in vehicular cloud computing, vehicular fog computing, vehicular edge computing, the Internet of Vehicles, the Internet of Things, mobile IPv6 security, and cryptography.

MOHAMED Y. DAHAB has been an Associate Professor at the Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University (KAU), Jeddah, Saudi Arabia, since 2010. He served as the Chairperson of the Agricultural Expert Systems Development Department, Central Laboratory for Agricultural Expert Systems (CLAES), Ministry of Agriculture, Egypt, for two years. His main research interests include algorithms, semantic web, pattern recognition, natural language processing, expert systems, knowledge bases, information extraction, and information retrieval.

FATHY E. EASSA received the B.Sc. degree in electronics and electrical communication engineering from Cairo University, Egypt, in 1978, and the M.Sc. and Ph.D. degrees in computers and systems engineering from Al-Azhar University, Cairo, Egypt, in 1984 and 1989, respectively. In 1989, he was a Joint Supervision with the University of Colorado, Boulder, CO, USA, and Al-Azhar University. He is currently a Full Professor with the Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia. His research interests include agent-based software engineering, cloud computing, software engineering, big data, distributed systems, and exactable system testing.

REDA SALAMA worked as a consultant at several computer software companies. He has been an Associate Professor at the Department of Information Technology, Faculty of Computing and Information Technology, King Abdul Aziz University (KAU), Jeddah, Saudi Arabia, since 2003. His main research interests include distributed systems, internet technologies, e-learning systems, and multimedia information retrieval systems.

SEIF HARIDI is currently the Chair Professor of computer systems specialized in parallel and distributed computing, and the Head of the Distributed Computing Group at the KTH Royal Institute of Technology, Stockholm, Sweden. He is also the Chief Scientific Advisor of RISE SICS, until December 2019. He led a European research program on cloud computing and big data at EIT-Digital, from 2010 to 2013. He is a co-founder of a number of start-ups in the area of distributed and cloud computing, including Hive Streaming and logical clocks, and a co-designer of SICStus Prolog, the most well-known logic programming system and the Mozart Programming System, a high-quality open-source development platform based on the Oz multi-paradigm programming language. His research interests include in the combination of systems research and theory in the areas of programming systems and distributed computing.

ABDULLAH S. AL-GHAMDI received the B.Sc. degree in computer science from The University of Southern Mississippi, Hattiesburg, MS, USA, in 1990, the M.Sc. degree in management information systems from the University of Illinois at Springfield, Springfield, IL, USA, in 1992, and the Ph.D. degree in computer science from George Washington University, Washington, DC, USA, in 2003. He is currently a Full Professor with the Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia. His research interests include collaborative software, distributed systems, conflict measurements, workflow, information systems, and artificial intelligence.