Big Data in Vehicular Cloud Computing: Review, Taxonomy, and Security Challenges

Majed S. Alsayfi[1, *], Mohamed Y. Dahab[1], Fathy E. Eassa[1], Reda Salama[2], Seif Haridi[3], Abdullah S. Al-Ghamdi[4]

[1]Department of Computer Science, Faculty of Computing and Information Technology, King Abdelaziz University, Jeddah 21589, Saudi Arabia

[2]Department of Information Technology, Faculty of Computing and Information Technology, King Abdelaziz University, Jeddah 21589, Saudi Arabia

[3]KTH Royal Institute of Technology, Stockholm, Sweden

[4]Department of Information System, Faculty of Computing and Information Technology, King Abdelaziz University, Jeddah 21589, Saudi Arabia

msalamahalsayfi@stu.kau.edu.sa

***Abstract*—Modern vehicles equipped with various smart sensors have become a means of transportation and have become a means of collecting, creating, computing, processing, and transferring data while traveling through modern and rural cities. A traditional vehicular ad hoc network (VANET) cannot handle the enormous and complex data that are collected by modern vehicle sensors (e.g., cameras, lidar, and global positioning systems (GPS)) because they require rapid processing, analysis, management, storage, and uploading to trusted national authorities. Furthermore, the integrated VANET with cloud computing presents a new concept, vehicular cloud computing (VCC), which overcomes the limitations of VANET, brings new services and applications to vehicular networks, and generates a massive amount of data compared to the data collected by individual vehicles alone. Therefore, this study explored the importance of big data in VCC. First, we provide an overview of traditional vehicular networks and their limitations. Then we investigate the relationship between VCC and big data, fundamentally focusing on how VCC can generate, transmit, store, upload, and process big data to share it among vehicles on the road. Subsequently, a new taxonomy of big data in VCC was presented. Finally, the security challenges in big data-based VCCs are discussed.**

***Index Terms*—Big data; Security; Traditional vehicular network; Vehicular cloud computing; On-board unit.**

I. INTRODUCTION

Automobile factories are seeking to develop autonomous vehicles to keep pace with technological developments around the world to provide better safety for drivers, passengers, and pedestrians. To achieve this, self-driving vehicles should first have effective computation, processing, and communication with the Internet to communicate with other vehicles. Fixed infrastructures, such as road site units (RSUs), and dynamic infrastructures, such as unmanned aerial vehicles (UAVs), are critical [1]. The authors of the studies in [2] and [3] stated that 50 billion things, including vehicles, will be online, generating 300,000 exabytes of data. This has led researchers to move from traditional vehicular networks (VANETs) to the Internet of Vehicles [4]–[6]. A VANET is defined as a type of mobile ad hoc network (MANET) that supports intelligent transportation systems (ITSs) on the road [7]–[9]. A VANET consists of three main components: vehicle, RSU, and traffic authority (TA). The RSU is responsible for the exchange of messages between the vehicles and the TA. The VANET components communicate with each other in two ways: vehicle-to-vehicle communication (V2VC) and RSU-to-vehicle communication (RSU2VC)/vehicle-to-RSU communication (V2RSUC) [10]–[12]. This is accomplished using the dedicated short-range communication (DSRC) protocols 4G-LTE [13], 5G [14], and 6G [15]. There is a lot of information exchanged between vehicles or between vehicles and infrastructures, such as accident notifications, accident avoidance, traffic jams, and road maintenance works, which can generate real-time, semi-real-time, and offline big data.

Furthermore, modern autonomous vehicles are equipped with various smart sensors [16], [17], such as cameras, global positioning systems (GPS), lights, tire pressure, A/C, temperature, and seat sensors. These smart sensors are located in the vehicle's on-board unit (OBU) [18], [19] and collect various data inside and outside the vehicle. Some simple data are processed inside the OBU, whereas other complex data are not. However, this complex information depends on powerful processing, particularly for real-time data, which requires rapid decision-making (e.g., capturing

Manuscript received 7 December, 2021; accepted 7 March, 2022.

This work was supported by the Deanship of Scientific Research (DSR), King Abdelaziz University (Jeddah, Saudi Arabia), under Grant No. KEP-PHD-21-611-42.

a video of a road accident). Consequently, new technologies have emerged to deal with such complex data. This technology is vehicular cloud computing (VCC), which integrates a traditional vehicular network (VANET) with cloud computing [20]–[22].

A VCC is defined as "a group of largely autonomous vehicles, whose corporate computing, sensing, communication, and physical resources can be coordinated and dynamically allocated to authorized users" [23]. This integration has led to VCC benefitting from VANETs and cloud computing. The main advantage of VCC is its ability to process complex big data in real time, semi-real time, and offline, as well as to provide new services and applications in vehicular network environments. Furthermore, OBU sensors collect a huge amount of data from different geographical locations on the road, store it in the vehicle OBU and share the stored data with other vehicles. However, this big data will bring a significant challenge to vehicle OBUs in VANETs, especially for real-time big data that require quick decision-making. Therefore, the VCC functions not only as a road travel assistance, but also as a local mobile storage centre that can be used to process urgent big data. The main contributions of this study are as follows:

– Providing a survey on the relationship between big data and VCC;
– Proposing a VCC taxonomy related to big data;
– Presenting the main challenges of big data transmission and storage in VCC;
– Outlining the security challenges of big data in VCC.

II. Related Works

This section presents studies that focus on big data in vehicular networks.

In [24], the authors presented a survey on big data analysis in the domain of intelligent transportation systems (ITS). They started this survey by providing a brief description of the history and characteristics of both big data analysis and ITS. In addition, they explored the big data analysis architecture in the ITS. This architecture consists of three layers: the data collection layer, data analytic layer, and application layer. Furthermore, this survey presents several big data applications in the ITS environment such as road traffic flow prediction, traffic accidents, vehicle maintenance, and rail transportation management. However, the proposed work did not show the impact of threats and attacks on big data in ITS, and big data in VCC have not been mentioned.

In [25], the authors presented a case study to analyse VANET measurement data to detect weak communication efficiency using a machine learning scheme. In addition, they classified the generation of big data in traditional networks (VANETs) as global position system (GPS) data, vehicle sensing data, self-driving related data, and vehicle mobile service data. They used 5G technology to transmit big data through networks. However, they mentioned the collection, processing, and analysis of big data in VCC.

The authors in [26] proposed a comprehensive review of big data in the transportation domain. The main objective of this review is to explore current research and challenges related to big data in transportation systems. Similarly, the authors in [27] presented a survey of big data analytics in the domain of railway transportation systems. However, neither works in [26] and [27] showed how to protect big data during transmission, nor did they mention big data in the VCC system.

In [28], the authors proposed a comprehensive survey on vehicular edge computing (VEC). This survey explores VEC architecture, VEC services and applications, intelligent vehicle concepts, and communication among vehicles. A comparison between VEC and VCC is presented based on several factors such as location, mobility, latency, and communication overhead. Moreover, they presented a VEC architecture consisting of three layers: vehicle, edge cloud, and remote cloud layers. Although this survey provides important high-level details about VEC, it did not present big data processing and analysis for VEC and VCC.

In [29], Prehofer and Mehmood presented a new architecture for analysing big data in vehicles. The main aim of this approach is to show the detailed level of vehicle services and analyse the time resolution at a fine-grained level. In addition, they compared their implementation in Spark and Flink based on several parameters, such as latency, throughput, computational model, and fault-tolerant overhead. Nevertheless, this approach did not show the data storage process in the OBU nor did it mention the VCC domain.

In [30], the authors proposed a comprehensive review of big data analysis and processing in the Internet of Vehicles (IoV) domain. They presented a new taxonomy of their approach, which was divided into four categories: data storage, acquisition, processing, and analysis. Moreover, the authors presented a big data processing architecture based on IoV which consists of six layers. These layers show the phases of data collection from data acquisition, data transformation, data normalisation, data storage, data processing, and analysis until they reach the decision-making layer. However, this review does not cover the importance of big data in all vehicular network environments, such as in the VCC era.

The authors in [31] produced a book on big data analytics in ITS. This book highlights the most important topics in the intelligent transportation domain, such as accident detection and location routing. The main motivation of this book is to provide valuable reference resources to engineers, academics, researchers, and students interested in big data analytics in vehicular networks. Big data on VCC have not been discussed.

Gu, Zeng, and Guo [32] provided a comprehensive survey of VCC. In this survey, the authors presented a new two-layer architecture based on the resources used in services. These include network as a service (NaaS), collaboration as a service (coaaS), storage as a service (StaaS), and sensing as a service (SaaS). However, security and privacy issues as well as big data processing and management were not mentioned.

Whaiduzzaman, Sookhak, Gani, and Buyya [33] proposed a comprehensive study of VCCs. They defined the concept of an integrated VANET with cloud computing to form VCC. Then they showed the importance of the VCC in

the ITS domain. In addition, they presented new services in VCC, such as information as a service (InaaS), entertainment as a service (EaaS), network as a service (NaaS), and computation as a service (Com aaS). However, the authors did not explore the big data generated by VCC services.

The authors in [34] proposed an overview of VCC and its security. They provide a brief description of traditional VANETs and VCCs and outline VCC architecture, applications, security challenges, and threats. Although this overview provides an excellent introduction to VCC, they did not discuss the big data generated by VCC applications.

The authors in [35] presented a VCC survey for road traffic management. They classified VCC into two types: vehicle-to-vehicle cloud (VVC) and vehicle-to-infrastructure cloud (VIC). Subsequently, a basic taxonomy of VCC is presented. However, big data analysis, processing, and management have not been discussed.

The authors in [36] proposed the concept of VCC by integrating a traditional VANET with remote cloud computing to enable self-driving vehicles to deal with new applications and services in the ITS environment. In addition, these self-dravings can share and exchange data generated by OBU's vehicles with other vehicles on the road. However, this approach did not show the processing and analytic big data in the OBU in the VCC environment.

Another study in [37] presented a survey on VCCs. The authors of this study proposed a VCC architecture and presented a new taxonomy for the management of VCC resources. These open issues are discussed below.

The authors in [38] have presented another VCC survey. In the review, they introduced the VCC architecture, services, and applications. They classified applications and services based on vehicle mobility and remote cloud computing dependency. However, big data was not considered in this review.

Similarly, the authors in [39] presented an overview of VCC. They began by providing a brief description and comparison between remote and mobile cloud computing. They then explored VCC services and applications as well as security and privacy challenges.

Another VCC survey was conducted by Jabbarpour, Marefat, Jalooli, and Zarrabi [40]. The authors divided VCC into three main types: vehicular that uses the cloud, vehicular as a cloud, and hybrid vehicular cloud. A comparison of these three types of VCCs is presented. However, big data on VCC has not been discussed.

Ahmed, Malik, Hafeez, and Ahmed [41] presented an overview of a VCC based on its services and simulation framework. They introduced services that could be used in VCC. In addition, they explored existing tools and simulators used to evaluate the performance of architectures for vehicular networks, such as traditional VANETs and VCCs. Although they discussed open issues and challenges in the VCC domain, they did not focus on the importance of big data.

In [42], Masood, Lakew, and Cho presented a comprehensive review of the security and privacy challenges in a connected VCC. This review begins by describing VANETs, cloud computing, and mobile cloud computing. They then provide a comparison between the VCC types: vehicular using cloud, vehicular cloud, and hybrid vehicular cloud. Although this study touched on important information on security and privacy challenges in vehicle computing, it did not consider the importance of big data processing analysis and the management of VCC.

Goumidi, Aliouat, and Harous [43] proposed a comprehensive survey of VCC. The main aim of a VCC is to move a traditional VANET toward autonomous self-driving. Moreover, they started by providing a description of concepts such as mobile cloud computing, cloud computing, VANET, and VCC, and the components among these concepts. The authors then outlined the services in VCC, such as a service (NaaS), sensing as a service (SaaS), cooperation as a service (CaaS), storage as a service (StaaS), and computation as a service (Coaas). They outlined new applications of VCC such as traffic management, disaster management, and autonomous driving management. Although this approach covers important information regarding security and privacy issues, it does not consider big data.

The authors in [44] presented a new survey study. They focused on data dissemination in VANETs using VECs and VCCs. They introduced a brief description of cloud computing, fog computing, VANET, VEC, and VCC, as well as the advantages and disadvantages of each concept. Moreover, the authors demonstrated the differences between VEC and VCC based on latency, storage capacity, mobility, and bandwidth. However, big data challenges in VCC have not been discussed.

The study of big data in VCC is a promising and thriving field. In this study, we presented an overview of big data in VCC and its security challenges. On the basis of the literature, we propose a new taxonomy for big data in VCC. As illustrated in Section IV, our proposed taxonomy is divided into five categories: application services for big data, transmission of big data, storage of big data, computing of big data, and big data security in VCC. Thus, there is a lack of studies that provide an overview of the services, transmission, storage, and security of big data applications in VCC. As a result, to the best of our knowledge, this work is the first paper that focuses on big data in a VCC environment.

III. BIG DATA IN VEHICULAR CLOUD COMPUTING (VCC)

The VCC is divided into three types: vehicles that use clouds, vehicles as clouds, and hybrid vehicular clouds [45].

A. Vehicular Using Cloud

A vehicular using cloud (VuC) refers to a vehicle that uses an OBU (Fig. 1) to collect data (e.g., driver status, passenger status, oil sensors, tire sensors, GPS sensor, camera sensors, and LiDAR sensor) and display data on accidents, traffic jams, traffic lights, and nearby vehicles on the driver/passenger mobile phone/tablet from inside or outside the vehicle. The data collected by the OBUs are processed locally, and then a copy is sent to the central cloud for storage after decision-making. As shown in Fig. 1, vehicles are equipped with various smart sensors, drivers, passengers, mobile phones, tablets, and sensors that

generate massive amounts of big data. The OBU of a vehicle transmits big data to the cloud through the RSU for storage, processing, and decision-making.

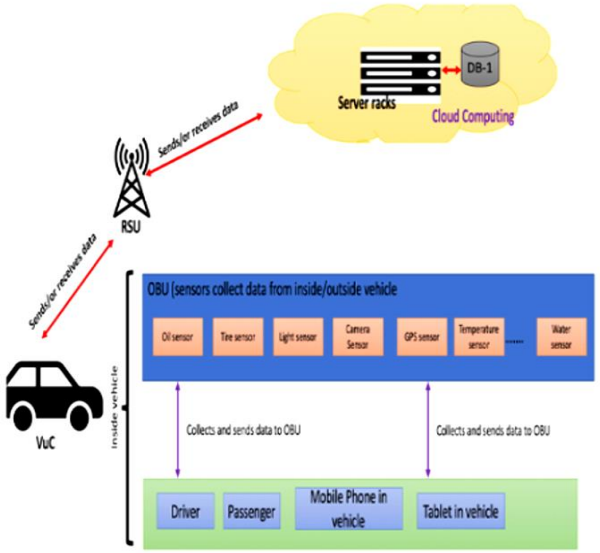

Fig. 1. Collecting data in VuC.

Internet connections and high-bandwidth connections between vehicles, infrastructure, and clouds are the main requirements for big data transmission. Currently, every modern vehicle is equipped with 100 sensors on average; this number will increase to more than 200 intelligent sensors that will generate more than 300 terabytes (TB) each year [46], [47]. Therefore, processing in-vehicle big data is one of the main challenges of VCC.

B. Vehicular as a Cloud

A vehicle as a cloud (VC) [33] is defined as a group of autonomous vehicles that exchanges, stores, and uploads valuable data on the road. A VC is launched when one of the group vehicles begins to form its own cloud by sending invitation messages to neighbouring vehicles to join the cloud on the road. Vehicles that receive invitation messages should forward them by accepting or rejecting them. After creating a VC, its members can act as storage clouds for these connections by sending, receiving, or processing data from other vehicles, RSUs, and clouds using DSRC, 4G-LTE, 5G, or 6G. Furthermore. VCs can be divided into two types [45]:

1. Static VC, where the members of the VC vehicles exchange big data in static mode;
2. Dynamic VC, where vehicles exchange and process data while moving on the road.

In addition, an electric autonomous vehicle cloud (EAVC) is not equipped with an engine; it only has an electrical battery for charging. Therefore, technology companies can use EAVC to install a powerful server with high storage capacity to process real-time data locally. However, sending real-time big data to the remote cloud for processing and decision-making may cause high latency during the long distance between the vehicle and the remote cloud. Therefore, VC will change the concept of vehicles from a means of transportation to a service provider or a local data centre for other vehicles on the road in modern and rural cities.

C. Hybrid Vehicular Cloud

A hybrid vehicular cloud (HVC) is a combination of a VuC and VC. Using this type of cloud, a vehicle can communicate through the simultaneous use of the VC and VuC. However, the HVC must first identify how the vehicle is responsible for computing, processing, sensing, sending, and receiving big data from member vehicles before forwarding information to the cloud. One of the approaches used in this scenario is the broker technique [48]. Using a broker in the HVC reduces duplicate messages on the broker's OBU, the overhead communication of the RSU, and cloud computing.

IV. A TAXONOMY FOR BIG DATA IN VEHICULAR CLOUD COMPUTING

VCC is a combination of traditional VANETs and cloud computing that provides new services to vehicular networks. These vehicles move daily on the road, generating a massive amount of big data sent to a remote cloud for storage. VCC may be a suitable environment for dealing with big data in edge networks, particularly for real-world data. A novel taxonomy of big data in VCC is presented in Fig. 2. This taxonomy consists of the application services of big data, transmission of big data, storage of big data, computing of big data, and big data security in VCC, which will be explained in the following sections.

A. Application Services of Big Data in VCC

Big data transmission is one of the main challenges in the VCC environment, due to the high mobility of vehicles. Big data in a VCC can be transmitted in different ways: V2V, vehicle-to-infrastructure (V2I), and VC-to-VC. Each of these ways transfers big data using a DSRC protocol, 4G-LTE, 5G, or 6G (in the future). Therefore, this section covers the following points.

1. Offline Application Services

Offline application services are responsible for collecting data, such as oil sensors, temperature sensors, tire sensors, brake sensors, gasoline sensors, etc., from inside vehicles [36]. These collected data produce big data stored in the OBU, without the need to upload them to the remote cloud.

2. Online Application Services

Online application services are responsible for collecting big data on the internet from the environment of a vehicle. These big data can include the status of a city at night, weather updates, etc. [49]. The data collected by vehicle sensors are massive and storing them in the OBU is insufficient. Because OBU storage is limited compared to remote cloud storage, OBU sends stored big data to the trusted authority department in the remote cloud to help improve and enhance road traffic, as well as for research and academic purposes.

3. Real-Time Application Services

Real-time application services are responsible for collecting sensitive information from inside and outside vehicles in real time. For example, when a vehicle is on the road, it can record an urgent event from inside the vehicle as a driver's status mode or outside the vehicle, such as a fire,

earthquake, flood, traffic jams, accident avoidance, criminals, or tornado, using its camera(s). These real-time data are then stored in the OBU, which transmits them to the cloud-trusted authority directly or via the RSU. Trusted authorities should make decisions concerning real-time data and update police officers with relevant details.

In [50], the authors proposed a new means of distributing digital advertisements in real time. This idea involves using particular public vehicles, such as taxis and buses, to distribute advertisements to vehicles on the road. Moreover, this method of advertising may reach numerous people while driving, especially if they are real advertisements in real time and not registered advertisements, thus changing the current commercial and governmental advertisements in the near future. However, this approach has some limitations, including OBU overhead, because the vehicle can receive more than one of the same digital advertisements simultaneously. As such, there is a need for self-driving cars dedicated to processing and displaying advertisements according to the region and the tendencies of people.

4. Discussion

These offline, online, and real-time applications generate enormous amounts of big data that require processing, filtering, storing, and uploading powerful datacentres. The OBUs of current vehicles find it difficult to manage this volume of data due to storage limitations. Therefore, the integration of cloud, fog and edge computing with OBUs is required to handle big data at the network edge. Table I shows a 4comparison between vehicular network types based on offline, online, and real-time application services of big data.

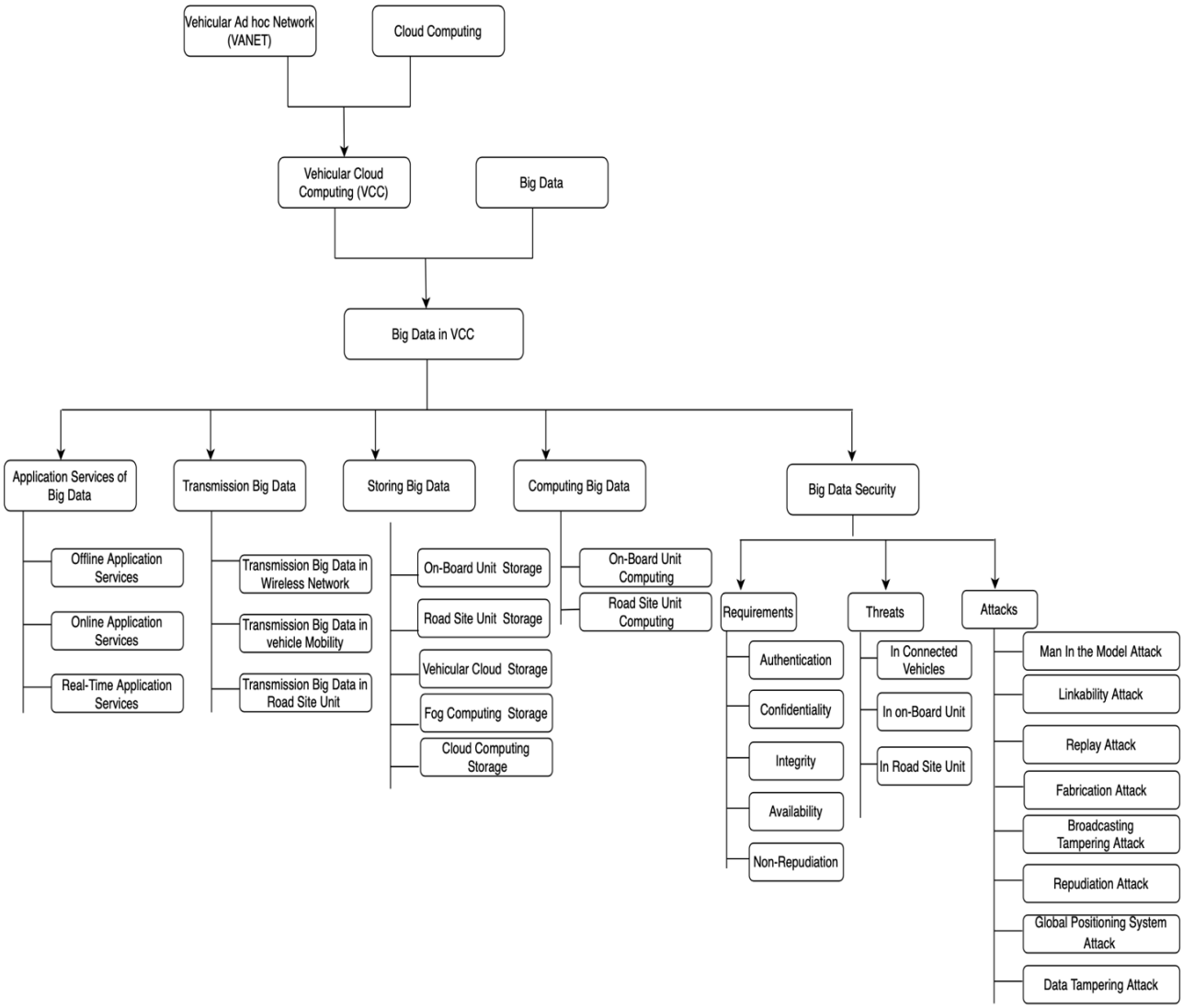

Fig. 2. A taxonomy of big data in VCC.

TABLE I. COMPARISON TABLE BETWEEN VEHICULAR NETWORK TYPE BASED ON APPLICATION SERVICES OF BIG DATA.

Application Services	**Vehicular Network Type**		
	VANET	**IoV**	**VCC**
Offline application services	√	√	√
Online application services	X	√	√
Real-Time application services	X	X	√

B. Transmission of Big Data in VCC

The exchange and transmission of big data in VCC environments is completely different from that in other environments because the former requires reliable and fast bandwidths for decision-making regarding urgent events in real time. Additionally, some factors may affect big data transmission in VCC environments, as shown in Fig. 3.

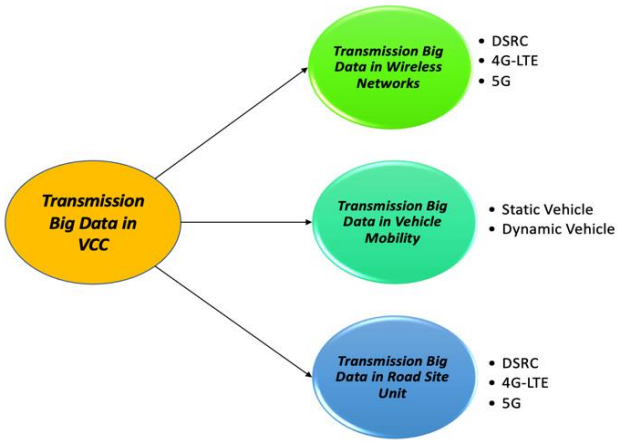

Fig. 3. Transmission of Big Data in VCC.

1. Transmission of Big Data in Wireless Networks

Vehicles communicate with each other wirelessly using the DSRC protocol, 4G-LTE [51] or 5G for data transmission between vehicles and the RSU or other vehicles. Moreover, there are barriers that prevent data from reaching their destination, such as buildings and bridges. To overcome these challenges, a new protocol design is required to transfer data smoothly between vehicles on the road.

2. Transmission of Big Data in Vehicle Mobility

A vehicle on the road has three states:

1. A static vehicle, which means that the vehicle is immobile. In this state, it is easy to manage and transmit big data between vehicles and RSUs;
2. Dynamic vehicles, which means that the vehicle is mobile (with normal speed) throughout the city;
3. High-dynamic vehicles, which means that the vehicle is travelling at high speeds.

Vehicle mobility is one of the main challenges in VCC when sending and receiving big data between vehicles or between vehicles and RSUs, particularly for real-time application services. This is because of short-range communication between vehicles. Moreover, the topology of a vehicle changes based on the number of vehicles on the road, that is, vehicles use the 802.11 protocol [52], which has limited coverage. As such, if one of the two vehicles (which is already communicating) moves out of range, it ceases to be able to exchange messages. This is the case where two vehicles are moving at a normal speed (e.g., 60 km/h). However, if vehicles travel at high speeds, the exchange or gathering of information from other vehicles becomes difficult due to the limited range of wireless communications in vehicular networks. This leads to difficulties in monitoring the road and recording critical events, such as accidents. One solution that may help to manage the effects of high vehicular speeds is to deploy RSUs along all roads to maintain active communication. However, this will undoubtedly incur high costs for governments in deploying groups of RSUs in modern cities and rural areas.

3. Transmission of Big Data in Road Site Unit

An RSU is a vehicular network component that communicates with other vehicles to avoid a short communication range between vehicles. The RSU covers approximately 6 km of road [53]. It is capable of transmitting big data to neighbouring RSUs to provide real-time information to drivers. However, if an RSU is absent or on the road, vehicles face major problems in transmitting big data through the DSRC protocol. This is because the DSRC requires the support of the RSU to transmit big data to the remote cloud. Thus, the design of an appropriate protocol is needed to work in heterogeneous access. Another solution involves using drivers/passengers' smartphones or tablets as access points to deliver data via 4G-LTE or 5G.

4. Discussion

Big data transmission is a challenge in VCC, because it requires an appropriate protocol to transfer data through different network layers. The current DSRC and 4G-LTE protocols suffer from scalability, mobility, and latency issues, which are mandatory requirements for big data transmission in VCC environments, especially services and applications that require quick decision-making from a country's trusted authority. Moreover, 5G is a promising technology that can be used to transmit big data in VCC due to its rapid data rates compared to 4G-LTE. However, there is a need to design a new intelligent protocol that transmits big data based on current network conditions because converting the entire network infrastructure from 4G to 5G (or 6G) is a difficult and expensive endeavour for governments [15], [54] in the future.

C. Storing Big Data in VCC

This section covers various methods for storing data in VCC. Figure 4 shows five types of data storage in a VCC: on-board storage units, road site unit storage, vehicular cloud storage, fog computing storage, and cloud computing storage.

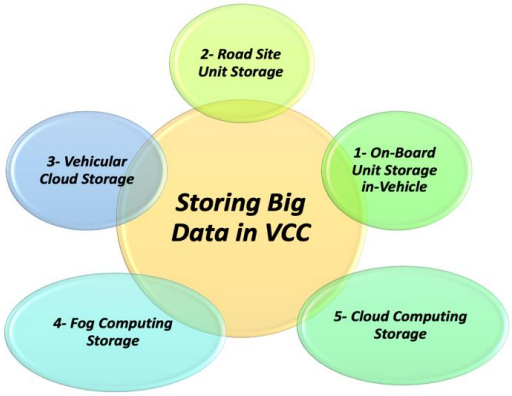

Fig. 4. Storing Big Data in VCC.

1. On-Board Unit Storage in-Vehicle

Each vehicle is equipped with an OBU. Each OBU consists of various sensors that collect data from inside and outside the vehicle and then store it in the OBU, the processing unit, and the communication unit [18]. The main aim of the OBU is to provide traffic authorities with information on vehicles. In addition, smart devices in vehicles, such as tablets, mobile phones, and watches, can be used to store vehicle data. Additionally, OBUs for old vehicles have limited storage, whereas modern vehicles are equipped with high storage. For example, Tesla [55] is an electric self-driving vehicle that does not have a machine engine as in traditional vehicles, making vehicle companies take advantage of this feature by providing high-performance computers to help other vehicles make decisions during transportation on the road. Therefore, a modern vehicle's OBU can store big data and rent a space for its OBU to other vehicles, such as a vehicle stopping in parking for a long period of time, and it can rent a specific area of its storage capacity in the OBU for a sum of money.

2. Road Site Unit Storage

The RSU is one of the components that shares information with the next RSU and the vehicles on the road. The RSU is equipped with its own storage, which is similar to that of the OBU, but the RSU is located on the road while the OBU is inside the vehicle. Furthermore, the RSU communicates with vehicles by exchanging safety and non-safety information about road status and vehicle information and then stores it in the RSU [56]. In [57], Kohda Wireless proposed a divisible RSU to communicate and store vehicle information details, as well as road event data. This is called "MK6C-EVK" which integrates board storage with a USB in a box in the RSU. Therefore, the RSU broadcasts the road status to all vehicles in its range, based on the information in its storage.

3. Vehicular Cloud Storage

A VC is one of the VCC type that enables a vehicle to create its own cloud on the road. The vehicle sends invitations (messages) to all neighbouring vehicles. This message consists of information about joining the cloud; the vehicle waits for all neighbouring vehicles to respond. If a neighbouring vehicle accepts this message, a VC is created. When creating a VC, VC members elect one of the vehicles to act as the vehicle leader. This vehicle leader should have a large storage capacity to manage and store all data received from its members. The primary goal of a VC is to make a vehicle leader a dynamic data centre on the road to receive, process, and share big data with its members and other entities in the network. Consequently, a sufficient protocol is required to achieve the VCC objectives.

4. Fog Computing Storage

Fog computing (FC) is a cloud with fewer capabilities than the traditional cloud [58], [59] storage. FC [60], [61] is located between the end user and the traditional cloud and is used to avoid the high latency involved in traditional cloud storage. FC aims to support mobility, security, privacy, and low latency for edge vehicles in a network. In addition, FC is suitable for real-time application services that require high processing and decision-making about real-world road events. Furthermore, in [62], the authors proposed an approach to integrate a vehicular network with an FC to form vehicular fog computing (VFC), describing the VFC architecture and its functions. However, this study did not mention how the big VFC data were transmitted. It is believed that VFC will play an important role in VCC big data; thus, much VFC research is required.

5. Cloud Computing Storage

Cloud computing is the backbone of VCC because it helps vehicles exchange complex data with each other through cloud computing. Cloud computing consists of three types: public, private, and hybrid [63]. Cloud computing modelling includes platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS). Cloud computing is widely used by companies, enterprises, and end users. This is because cloud computing has a massive number of data centres that can provide services to users anytime and anywhere via the internet. Consequently, the vehicle uses cloud computing to store and upload big data collected on the road.

6. Discussion

One of the challenges in storing big data in a VCC is scheduling, processing, and computing big data by an OBU. The OBU collected sensor-based data; some of these data were high priority and required real-time processing. The delivery of big data in a VCC is extremely complex because of the high mobility of vehicles and the varying locations at any time. Consequently, autonomous electric vehicles can achieve the vision of a VCC data centre on the road. However, this comes with inherent risks of possibly losing big data if the mobile VCC data centre was to get into an accident.

D. Computing Big Data in VCC

In 1968 [64], the Volkswagen Group presented the first vehicular computer controller called the "electronic fuel injector" (EFI). In 1969, the Ford Motor Company introduced the first device controller in vehicles [65]. In 1973, Chrysler applied an engine control unit (ECU) to vehicles [64]. In 1975, an ECU was available for all vehicles in the United States [64]. Initially, the ECU focused on processing data collected by the sensors. However, the concept of ECUs has changed because vehicles are equipped with numerous sensors, which enable V2V and V2I communication. Communication between V2V and V2I requires powerful computations.

In [57], several devices with different capabilities were provided to handle the data generated by vehicles and RSUs on the road that could be implemented in OBUs and RSUs in VCC. The authors of [66] proposed a platoon for vehicles. This approach aims to reduce OBU overhead and improve reliability. Several approaches have focused on improving the OBU processing of intervehicular communication and sensor data [67]–[69]. Olariu, Hristov, and Yan [70] proposed a new service called "computation as a service" (CaaS). Therefore, the OBU computation plays an important role in the processing of big data from autonomous vehicles in VCC. As such, modern OBUs should be able to process 25 TB per month [47], which requires powerful OBU storage capabilities in vehicles.

E. Big Data Security in VCC

Big data generated from vehicles in a VCC should be protected against internal and external attackers, because any modification in these data will affect the decision taken by traffic authorities, especially for real-time applications and services. VCC inherits the security and privacy issues from VANETs [21] and cloud computing. Moreover, big data security in VCC will play an important role in the future as vehicles gain the ability to generate more than 250 TB of data per year [47]. Notably, VCC big data security is more difficult than that of other systems because it is based on factors such as mobility, availability, latency, and storage capacity.

The authors in [34] presented a comprehensive survey of VCC after reviewing its architecture, security, and privacy. They outlined the factors that affect security and how vehicles communicate with other vehicles on the road. However, this study did not focus on big data security solutions in VCC. The authors in [21], who described possible attacks on VCC and presented security challenges that should be considered when designing the VCC architecture, analysed security and privacy. However, big data was not considered in this study.

A new service, called "traffic as a service" (TaaS), was presented by the authors in [71]. This service monitors vehicles and records traffic information on the roads. Traffic information is distributed to all vehicles through vehicles or RSUs on the road to take another path in the case of accidents or traffic jams. Finally, a large amount of information is uploaded to the cloud. However, the big data generated from traffic information are not secure and can be manipulated by intruders while sent to other vehicles or RSUs.

The authors in [72] proposed a new VCC service that aims to collect traffic information by recording videos and taking pictures using a vehicle camera. This service is called the "picture-on-wheel (POW) service". As the vehicle moves through the city, its camera enables the collection of traffic information by capturing real-time pictures or video recordings and sending them to the TA department in the cloud. The TA department then notifies all vehicles of the status of the road every few seconds. However, big data security issues have not been addressed using this approach.

Accordingly, the authors of [73] proposed a method to overcome the limitations of [72]. The approach consists of two tiers: a cloud tier and a vehicle tier. In this study, we propose a new service called Witness as a Service (WaaS). This service monitors road events. When a vehicle encounters an event on the road, such as an accident, it turns on its camera and begins to record the accident. Subsequently, a video is sent to the TA department for cloud computing. Before sending the video to the TA department, the vehicle's OBU encrypts the video using two asymmetric methods: Elgamal [74] and elliptic curve encryption [75]. Video recording encryption via two cryptography techniques causes computational overhead from OBU. This is because these two cryptography techniques require a high level of computation and video recording. However, this study suffers from the problem of big data being distributed among high-mobility vehicles.

In [76], the authors proposed three tiers of architecture: the cloud computing tier, the RSU tier, and the vehicle tier. They mentioned the security requirements in the architecture design. However, they did not mention how the data were transferred between the tiers.

Recently, the authors in [77] proposed a new method for securing data, called "vehicle pseudonyms". The idea behind this method is that the vehicle generates its own pseudonymous name and then sends it to the TA department to obtain permission to initiate communication between vehicles and RSUs on the road. However, each pseudonymous name has a lifetime, which means that the OBU will have revoked the big data on pseudonymous names. This revoked pseudonymous name big data affects the processing and computing traffic of information because of the storage limitations of the OBU.

The authors in [78] proposed two architecture tiers using 5G communication: the cloud tier and the vehicle tier, which can communicate with each other via millimeter wave technology. In addition, this approach presents a new service called "video reporting as a service" (RaaS). The vehicle records any event that occurs on the road using its camera and then sends it to the TA department. The TA department then processes the video and stores it on cloud computing. Several encryption techniques have been used to secure the data sent between vehicles and the TA department. The sent video recordings were sent to the TA department without delay. Consequently, the data sent from vehicles and received by the TA department, as well as the decision-making message regarding the recorded events, will generate big data, which require fast bandwidths to transmit between entities and protection from possible network attackers.

In VCC, big data security is divided into three main points: big data security requirements, big data security threats, and big data security attacks. These are discussed below.

1. Big Data Security Requirements in VCC

Several security requirements must be satisfied to secure big data in a VCC environment, as shown in Fig. 5.

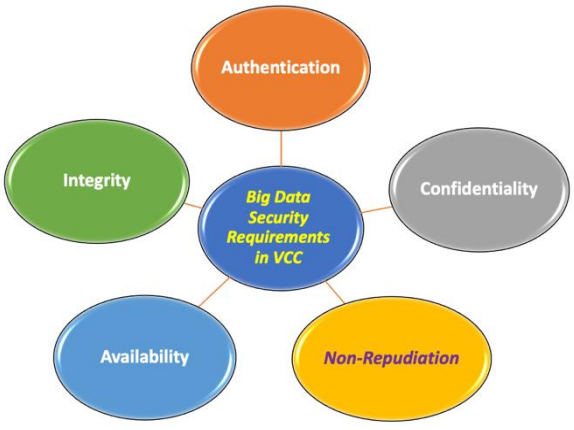

Fig. 5. Big data Security Requirements in VCC.

– *Authentication:* This ensures that the message is sent from a legitimate vehicle to a trusted destination using its

identity, biometrics, or tokens. During the high mobility of vehicles in VCC, the authentication process is a major challenge that should be considered when designing a security protocol to protect big data in VCC.

– *Confidentiality:* It means big data that is sent among vehicles, or vehicle and infrastructure may consist of sensitive information that should be protected against adversary. Digital signatures alone are insufficient to ensure confidentiality. It is mandatory to sign and encrypt messages to ensure that protected big data is transmitted among trusted entities in a VCC environment.

– *Integrity:* Big data should be received by trusted entities (vehicles, RSU, or traffic authorities) without alteration. Timestamps, random numbers, hashing, and nonce are techniques that can be used to satisfy this requirement.

– *Availability:* Data should be available to vehicles when needed. Certain safety applications, such as accident notifications and city monitoring, require real-time or near-real-time communication. A single millisecond delay renders the message meaningless and the consequences can be devastating.

– *Non-Repudiation:* This means that any trusted entity (vehicle or RSU) should not deny sending or receiving the data originating from it.

2. Big Data Security Threats in VCC

Vehicles use intelligent sensors to collect sensitive and insensitive data from the surrounding environment while moving on a road. This amount of recorded data is stored in the OBU. An OBU is one of the places in vehicles that intruders target to obtain data and use it illegally, which slows the network and delays data transmission between vehicles and RSUs. Another entity that might be attacked is the Tamper Proof Device (TPD) which stores private and public keys for encryption and decryption messages. TPD is considered one of the most important points for intruders to initiate communication with legitimate vehicles and exchange important information related to safety applications such as traffic accidents. Moreover, RSUs are important entities in vehicular networks that are located among vehicles and traffic authorities to exchange valuable data among them. This entity is one of the most important things that intruders seek to control to exchange data with vehicles and traffic authorities, as well as to store and use these data illegally. Therefore, to ensure the secure transmission of big data, the vehicle, the RSU, and the traffic authority must be fully protected against intruders.

3. Big Data Security Attacks in VCC

There are several attacks on big data vehicles during transmission in VCC environments. These attacks are categorised into several categories as follows:

– *Man-in-the-Middle Attack:* This attack aims to intercept the communication between vehicles, RSUs, and traffic authorities when transmitting big data on a network without prior knowledge of whether the big data originate from a legitimate or fake entity.

– *Linkability Attack:* This attack aims to link multiple link big data processing, big data analysis, big data uploading, and pseudonymous identities for vehicles and RSUs.

– *Replay Attack:* This attack aims to record big data, such as transmission among vehicles and RSUs, and copy it to use later.

– *Fabrication Attack:* This attack aims to send fabricated big data on crucial events, such as traffic accidents that occur on the road, to trusted vehicles, RSUs, and traffic authorities in the country and other trusted vehicles.

– *Broadcasting Tampering Attack:* This attack aims to send false indications to vehicles that there are any events on the road and that another road must be taken to avoid this event, even though there is nothing on the road.

– *Repudiation Attack:* This attack aims to plan to participate in big data transactions in the network and then deny participation in this transaction.

– *Global Positioning System Attack:* This attack aims to create a false location for vehicles to move incorrectly by spoofing GPS information through GPS satellite communication.

– *Data Tampering Attack:* This attack aims to perform an untrusted vehicle, RSUs, or traffic authorities to modify big data when transmission between legitimate entities through a network.

Finally, Table II shows a comparison of the approaches based on several important points: vehicular cloud type, cloud computing, fog computing, big data analysis, big data management, big data storage in OBU, security privacy, mobility, communication type, and machine learning requirements. However, these points are important for the delivery of big data from vehicles and infrastructure in a VCC environment.

TABLE II. A COMPARISON TABLE BETWEEN PREVIOUS WORKS. (√): FULLY ACHIEVED; (*): PARTIALLY ACHIEVED; (X): NOT ACHIEVED.

Ref.	Vehicular Network Type	Cloud Computing	Fog Computing	Big Data			Security	Privacy	Mobility	Communication Type	Machine Learning
				Big data Analysis	Big Data Management	Big Data Storage in OBU					
[21]	VCC	√	X	X	X	X	√	X	X	DSRC	X
[24]	VANET	√	X	√	√	*	X	X	X	DSRC	√
[25]	VANET	√	X	√	√	*	X	X	*	5G	√
[26]	VANET	*	X	√	√	*	X	X	X	DSRC	√
[29]	VANET	√	√	√	√	√	X	X	*	4G/5G	√
[30]	VANET	√	√	√	√	*	√	X	√	DSRC/4G/5G	√
[31]	IoV	√	√	√	√	√	√	√	*	DSRC/4G	√
[32]	VCC	√	X	X	X	X	X	X	*	DSRC/4G	X

Ref.	Vehicular Network Type	Cloud Computing	Fog Computing	Big Data			Security	Privacy	Mobility	Communication Type	Machine Learning
				Big data Analysis	Big Data Management	Big Data Storage in OBU					
[33]	VCC	√	X	X	X	X	*	*	*	DSRC/4G	X
[34]	VCC	√	X	X	X	X	*	*	X	DSRC/4G	X
[35]	VCC	√	√	X	X	X	X	X	*	DSRC/4G-LTE	X
[36]	VCC	√	X	X	X	X	X	X	*	DSRC/4G-LTE	X
[37]	VCC	√	X	X	X	X	X	X	√	4G	X
[38]	VCC	√	X	X	X	X	X	X	√	DSRC/4G	X
[39]	VCC	√	√	X	X	X	X	X	*	DSRC/4G	X
[40]	VCC	√	X	X	X	X	X	X	√	DSRC	X
[41]	VCC	√	X	X	X	X	X	X	√	DSRC/4G/5G	√
[42]	VCC	√	√	X	X	X	√	√	√	DSRC/4G	√
[43]	VCC	√	√	X	X	X	√	√	√	DSRC/4G	X
[44]	VCC	√	√	X	X	X	*	*	√	DSRC/4G	X
[71]	VANET	√	X	X	X	X	*	*	X	4G	X
[73]	VANET	√	√	X	X	X	√	√	X	4G	X
[76]	VCC	√	√	X	X	X	*	X	*	DSRC	X
[77]	VCC	√	√	X	X	X	√	√	X	DSRC	X

V. BIG DATA SECURITY CHALLENGES IN VCC

Security and privacy are major challenges in VCC for protecting big data while transmitting data between entities on networks. The main security challenges are as follows.

A. High Mobility Authentication

Authentication is a security requirement that plays an important role in VCC. In a VCC, the vehicle and RSU should be authenticated before sending messages between them. Vehicle authentication in a VCC has three phases: static vehicle authentication, dynamic vehicle authentication, and high dynamic vehicle authentication. Highly dynamic vehicle authentication is a challenge faced by VCCs. This is because the vehicle location changes every few seconds, which requires continuous authentication for every move. Consequently, a new security mechanism is required to manage VCC mobility and provide a strong cryptographic authentication technique.

B. Big Data Integrity

Big data sent between vehicles or between vehicles and RSUs can be manipulated by network intruders. Ensuring the authenticity of VCC big data is mandatory because of its sensitivity of the big data. As a result, new hashing techniques are required to protect data origin from internal and external network attacks, as well as quantum attacks [79].

C. Big Data Confidentiality

Vehicles and RSUs generate and exchange big data with each other vehicles and RSUs. Big data can be normal or urgent. Essentially, normal data do not require any action from the TA department; in contrast, urgent data require urgent, real-world decision-making. To provide big data confidentiality, the urgent data sent by vehicles/RSUs to the TA department are highly sensitive and should use symmetric or asymmetric algorithms to encrypt the data against intruders. Therefore, lightweight cryptography is required to avoid the OBU computation overhead.

D. Secure Vehicle Location

One of the challenges in VCC is location protection, particularly for real-time big data applications and services. Concurrently, real-time big data must send the exact locations of events that occur on the road. These locations will help police vehicles and ambulances arrive quickly in emergency situations. As a result, a new technique is required to protect the location of the vehicle and its location from internal and external intruders.

VI. FUTURE DIRECTION AND OPEN ISSUES

The number of smart electronic devices, such as mobile phones and tablets, as well as intelligent autonomous vehicles, will increase in the coming years as these devices will automatically connect to each other without human intervention. This will lead to the creation of huge amounts of big data, some of which are highly sensitive and require rapid processing and decision-making in real time. Integrating FC and edge computing with VCC, artificial intelligence (AI) [80] and machine learning (ML) [81] can be considered solutions for dealing with such big data in VCC. This integration will play an important role in reducing the burden on cloud computing, as well as avoiding the long distances between them, especially for big data that requires urgent decision-making. Moreover, a flexible and robust VCC architecture is needed to support massive inflation in big data because of the large number of intelligent autonomous vehicles that will connect with each other in the near future as the VCC becomes a local data centre on the road to store and process real-time data and make decisions. Therefore, a few authors have worked on VCC; they focused only on data offloading and data security in transit. However, they did not mention the importance of big data in VCC.

Despite significant progress in big data analytics, there are still many unresolved challenges that need to be addressed in future research. This section outlines some of the main challenges in utilising big data in VCC.

A. Data Collection

Due to the frequent and rapid movement of vehicles, the data collected in the VCC may be incomplete or inaccurate for a particular location. This is because such vehicles are not embedded in the advanced technologies required to provide real-time data, such as critical events, event locations, and vehicle locations on the road. Vehicle manufacturers should tackle this problem by developing powerful data collection technology. Thus, vehicles can collect important and sensitive data that can help traffic authorities develop roads and maintain traffic safety. Therefore, a new mechanism for collecting sensitive big data in real-time in a VCC environment is required.

B. Data Privacy

Privacy is considered one of the main challenges in the big data era in VCC. This is due to the privacy of big data that might be leaked during transmission in the VCC environment. Vehicle location can be easily collected by intruders if location data are not fully protected. Therefore, privacy protection is an important aspect of Big Data in VCC environments. Moreover, to prevent access to personal private information, traffic authorities must develop complete data privacy regulations that include what data can and cannot be published, as well as the scope of data dissemination and use. Therefore, traffic authorities must use smarter and more advanced algorithms to develop and improve the level of security of big data in VCC environments.

C. Data Storage

The volume of data has increased significantly in recent years. This acceleration in data increase preceded the development of high storage capacities to save data, especially in VCC. Vehicles produce a massive amount of data recorded through smart sensors that are stored in the OBU. However, the OBU does not have a large storage capacity to save all this data. For this, it uploads these massive amounts of data to fog computing or cloud computing and then references them when needed. Consequently, vehicle manufacturers should play an important role in data storage inside vehicles by developing highly efficient OBU storage systems linked to artificial intelligence and machine learning.

D. Data Processing

Vehicles generate big data recorded through intelligent sensors and store it in the OBU. These data require quick real-time processing, so any delay in this processing will lose the effectiveness and importance of these data. When these data are sent to cloud computing for processing and decision-making, they suffer from high latency because fog computing is one of the solutions to reduce this latency. However, important data, such as traffic accidents and the monitoring of criminal processing inside vehicles, will significantly solve the problems of latency and communication overhead in both fog and cloud computing. As a result, in VCC, vehicles elect one of the vehicles to become a cluster. This cluster receives vehicle data and divides it among the vehicles in the VCC for processing and feedback to the cluster. Subsequently, the cluster uploads data for storage in the fog or cloud computing.

The following points outline the future direction and open issues in the context of big data in VCC that may help researchers in the VCC domain focus on it:

– Need to deploy a successful VCC architecture to support big data;

– There is a need to increase the capacity of OBUs to handle massive amounts of big data in the future;

– Need to provide a high-bandwidth communication for real-time big data applications.

VII. CONCLUSIONS

In the near future, VCCs will play an important role in intelligent transportation systems. Modern autonomous vehicles (AVs) are equipped with thousands of intelligent sensors that generate large amounts of big data. Some of these big data require real-time processing and decision-making, which cannot be performed by traditional vehicular networks. This article provides a survey on dealing with big data using VCC. First, it explains why an integrated vehicular network with cloud computing is required. Second, the types of VCCs and how they communicate with other vehicles and RSUs on the road were presented. Third, a novel taxonomy is presented based on big data in VCCs. The relationships between big data and VCC are then presented in different categories, including storage, computing, processing, transmission, and security. Finally, this study reviewed the most prominent challenges in each classification that require further investigation and research. This survey provides an overview of big data in VCC that may help academic researchers, researchers, and industries.

ACKNOWLEDGMENT

The authors thank the Deanship of Scientific Research for providing the Technical support.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] K. P. Valavanis and G. J. Vachtsevanos, *Handbook of Unmanned Aerial Vehicles*. Dordrecht, Netherlands: Springer, 2015. DOI: 10.1007/978-90-481-9707-1_96.

[2] D. Evans, “The internet of things: How the next evolution of the internet is changing everything”, Cisco, 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] W. Xu *et al.*, “Internet of vehicles in big data era”, *IEEE/CAA J. Automatica Sinica*, vol. 5, no. 1, pp. 19–35, Jan. 2018. DOI: 10.1109/jas.2017.7510736.

[4] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, “An overview of internet of vehicles”, *China Commun.*, vol. 11, no. 10, pp. 1–15, Oct. 2014. DOI: 10.1109/cc.2014.6969789.

[5] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, “Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds”, in *Proc. of 2014 IEEE World Forum Internet Things (WF-IoT)*, 2014, pp. 241–246. DOI: 10.1109/WF-IoT.2014.6803166.

[6] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, “Routing in internet of vehicles: A review”, *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015. DOI: 10.1109/tits.2015.2423667.

[7] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*. Chichester: Wiley, 2010. DOI: 10.1002/9780470740637.

[8] S. Yousefi, M. S. Mousavi, and M. Fathy, “Vehicular ad hoc networks

(VANETs): Challenges and perspectives", in *Proc. of 2006 6th Int. Conf. ITS Telecommun.*, 2006, pp. 761–766. DOI: 10.1109/ITST.2006.289012.

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

[10] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta, "Empirical determination of channel characteristics for DSRC vehicle-to-vehicle communication", in *Proc. of 1st ACM Int. Workshop Veh. Ad Hoc Networks-VANET'04*, 2004, p. 88. DOI: 10.1145/1023875.1023890.

[11] J. Miller, "Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture", in *Proc. of 2008 IEEE Intell. Vehicles Symp.*, 2008, pp. 715–720. DOI: 10.1109/IVS.2008.4621301.

[12] C.-M. Chou, C.-Y. Li, W.-M. Chien, and K.-c. Lan, "A feasibility study on vehicle-to-infrastructure communication: WiFi vs. WiMAX", in *Proc. of 2009 10th Int. Conf. Mobile Data Manage. Syst. Services Middleware*, 2009, pp. 397–398. DOI: 10.1109./MDM.2009.127.

[13] 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, art. ID 2750452, 2017. DOI: 10.1155/2017/2750452.

[14] Q.-V. Pham *et al.*, "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.

[15] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems", *IEEE Netw.*, vol. 34, no. 3, pp. 134–142, May/Jun. 2020. DOI: 10.1109/mnet.001.1900287.

[16] N. Soni, R. Malekian, D. Andriukaitis, D. Navikas, "Internet of. vehicles based approach for road safety applications using sensor technologies", *Wireless personal communications*, vol. 105, iss. 4, pp. 1257-1284, 2019. DOI: 10.1007/s11277-019-06144-0.

[17] K. Jo, K. Chu, and M. Sunwoo, "Interacting multiple model filter-based sensor fusion of GPS with in-vehicle sensors for real-time vehicle positioning", *IEEE Trans. Intel. Transp. Syst.*, vol. 13, no. 1, pp. 329–343, Mar. 2012. DOI: 10.1109/tits.2011.2171033.

[18] 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. Advances in Intelligent Systems and Computing*, vol. 1257. Springer, Singapore, 2021. DOI: 10.1007/978-981-15-7907-3_15.

[19] V. Kumar, S. Mishra, and N. Chand, "Applications of VANETs: Present & future", *Commun. Netw.*, vol. 5, no. 1B, pp. 12–15, Jan. 2013. DOI: 10.4236/cn.2013.51B004.

[20] M. Gerla, "Vehicular cloud computing", in *Proc. of 2012 11th Annu. Mediterranean Ad Hoc Netw. Workshop (Med-Hoc-Net)*, 2012, pp. 152–155. DOI: 10.1109/MedHocNet.2012.6257116.

[21] 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, Mar. 2013. DOI: 10.1109/TITS.2012.2211870.

[22] 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.

[23] S. Olariu, M. Eltoweissy, and M. Younis, "Towards autonomous vehicular clouds", *ICST Trans. Mobile Commun. Appl.*, vol. 11, nos. 7–9, p. e2, Sep. 2011. DOI: 10.4108/icst.trans.mca.2011.e2.

[24] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey", *IEEE Transactions on Intelligent Transportation Systems.*, vol. 20, pp. 383–398, Jan. 2019. DOI: 10.1109/TITS.2018.2815678.

[25] N. Cheng, F. Lyu, J. Chen, W. Xu, H. Zhou, S. Zhang, and X. Shen, "Big data driven vehicular networks", *IEEE Network*, vol. 32, no. 6, pp. 160–167, Nov./Dec. 2018. DOI: 10.1109/MNET.2018.1700460.

[26] A. Neilson, Indratmo, B. Daniel, and S. Tjandra, "Systematic review of the literature on big data in the transportation domain: Concepts and applications", *Big Data Research.*, vol. 17, pp. 35–44, Sep. 2019. DOI: 10.1016/j.bdr.2019.03.001.

[27] F. Ghofrani, Q. He, R. M. P. Goverde, and X. Liu, "Recent applications of big data analytics in railway transportation systems: A survey", *Transportation Research Part C: Emerging Technologies*, vol. 90, pp. 226–246, May 2018. DOI: 10.1016/j.trc.2018.03.010.

[28] S. Raza, S. Wang, M. Ahmed, and M. R. Anwer, "A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions", *Wireless Communications and Mobile Computing*, vol. 2019, pp. 1–19, Feb. 2019. DOI: 10.1155/2019/3159762.

[29] C. Prehofer and S. Mehmood, "Big data architectures for vehicle data analysis", in *Proc. of 2020 IEEE International Conference on Big Data (Big Data)*, 2020, pp. 3404–3412. DOI: 10.1109/BigData50022.2020.9378397.

[30] A. Arooj, M. S. Farooq, A. Akram, R. Iqbal, A. Sharma, and G. Dhiman, "Big data processing and analysis in internet of vehicles: architecture, taxonomy, and open research challenges", *Archives of Computational Methods in Engineering*, vol. 29, pp. 793–829, 2022. DOI: 10.1007/s11831-021-09590-x.

[31] R. S. Rao, N. Singh, O. Kaiwartya, and S. Das, *Cloud-Based Big Data Analytics in Vehicular Ad-Hoc Networks*. IGI Global, 2020. DOI: 10.4018/978-1-7998-2764-1.

[32] L. Gu, D. Zeng, and S. Guo, "Vehicular cloud computing: A survey", in *Proc. of Globecom Workshops (GC Wkshps)*, 2013, pp. 403–407. DOI: 10.1109/GLOCOMW.2013.6825021.

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

[34] M. K. Sharma and A. Kaur, "A survey on vehicular cloud computing and its security", in *Proc. of 2015 1st International Conference on Next Generation Computing Technologies (NGCT)*, 2015, pp. 67–71. DOI: 10.1109/NGCT.2015.7375084.

[35] I. Ahmad, R. M. Noor, I. Ali, and M. A. Qureshi, "The role of vehicular cloud computing in road traffic management: A survey", *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering - Future Intelligent Vehicular Technologies*, pp. 123–131, 2017. DOI: 10.1007/978-3-319-51207-5_12.

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

[37] T. Mekki, I. Jabri, A. Rachedi, and M. ben Jemaa, "Vehicular cloud networks: Challenges, architectures, and future directions", *Veh. Commun.*, vol. 9, pp. 268–280, 2017. DOI: 10.1016/j.vehcom.2016.11.009.

[38] A. Boukerche and R. E. De Grande, "Vehicular cloud computing: Architectures, applications, and mobility", *Computer Networks*, vol. 135, pp. 171–189, 2018. DOI: 10.1016/j.comnet.2018.01.004.

[39] A. Ghazizadeh and S. Olariu, "Vehicular clouds: A survey and future directions", in *Cloud Computing for Optimization: Foundations, Applications, and Challenges. Studies in Big Data*, vol. 39. Springer, Cham, 2018. DOI: 10.1007/978-3-319-73676-1_17.

[40] M. R. Jabbarpour, A. Marefat, A. Jalooli, and H. Zarrabi, "Couldbased vehicular networks: A taxonomy, survey, and conceptual hybrid architecture", *Wireless Networks*, vol. 25, no. 1, pp. 335–354, 2019. DOI: 10.1007/s11276-017-1563-5.

[41] B. Ahmed, A. W. Malik, T. Hafeez, and N. Ahmed, "Services and simulation frameworks for vehicular cloud computing: A contemporary survey", *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, art. no. 4, pp. 1–21, 2019. DOI: 10.1186/s13638-018-1315-y.

[42] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing", *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2725–2764, 2020. DOI: 10.1109/COMST.2020.3012961.

[43] H. Goumidi, Z. Aliouat, and S. Harous, "Vehicular cloud computing security: A survey", *Arabian Journal for Science and Engineering*, vol. 45, pp. 2473–2499, 2020. DOI: 10.1007/s13369-019-04094-0.

[44] N. Gaouar and M. Lehsaini, "Toward vehicular cloud/fog communication: A survey on data dissemination in vehicular ad hoc networks using vehicular cloud/fog computing", *International Journal of Communication System*, vol. 34, no. 13, p. e4906, Sep. 2021. DOI: 10.1002/dac.4906.

[45] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging VANET with cloud computing", in *Proc. of 4th IEEE Int. Conf. Cloud Comput. Technol. Sci.*, 2012, pp. 606–609. DOI: 10.1109/CloudCom.2012.6427481.

[46] Automotive sensors and electronics expo 2017, In Vision Artificial Intelligence. [Online]. Available: https://invision.ai/2017-automotive-sensors-and-electronics-expo/

[47] S. Wright, "Autonomous cars will generate more than 300 TB of data per year", Tuxera. [Online]. Available: https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/

[48] M. Soyturk, K. N. Muhammad, M. N. Avcil, B. Kantarci, and J. Matthews, "Chapter 8 - From vehicular networks to vehicular clouds

in smart cities", *Smart Cities and Homes*, pp. 149–171, 2016. DOI: 10.1016/B978-0-12-803454-5.00008-0.
[49] G. Yan, D. B. Rawat, and B. B. Bista, "Towards secure vehicular clouds", in *Proc. of 2012 6th Int. Conf. Complex Intell. Softw. Intensive Syst.*, 2012, pp. 370–375. DOI: 10.1109/CISIS.2012.96.
[50] 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, Jun. 2016. DOI: 10.1109/TPDS.2015.2467392.
[51] J. Choi, V. Va, N. Gonzalez-Prelcic, R. Daniels, C. R. Bhat, and R. W. Heath, "Millimeter-wave vehicular communication to support massive automotive sensing", *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 160–167, Dec. 2016. DOI: 10.1109/MCOM.2016.1600071CM.
[52] A. Shaheen, A. Gaamel, and A. Bahaj, "Comparison and analysis study between AODV and DSR routing protocols in VANET with IEEE 802.11_b", *J. Ubiquitous Syst. Pervasive Netw.*, vol. 7, no. 1, pp. 7–12, 2016. DOI: 10.5383/JUSPN.07.01.002.
[53] G. Charalampopoulos, T. Dagiuklas, and T. Chrysikos, "V2I applications in highways: How RSU dimensioning can improve service delivery", in *Proc. of 2016 23rd Int. Conf. Telecommun. (ICT)*, 2016, pp. 1–6. DOI: 10.1109/ICT.2016.7500438.
[54] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6G: AI empowered wireless networks", *IEEE Commun. Mag.*, vol. 57, no. 8, pp. 84–90, Aug. 2019. DOI: 10.1109/MCOM.2019.1900271.
[55] M. Eberhard and M. Tarpenning, "The 21st Century Electric Car Tesla Motors", Palo Alto, CA, Tesla Motors, 2006.
[56] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks", in *Proc. of 2008 IEEE Int. Conf. Commun.*, 2008, pp. 1451–1457. DOI: 10.1109/ICC.2008.281.
[57] Hardware, Cohda Wirless. [Online]. Available: https://cohdawireless.com/solutions/hardware/
[58] B. Hayes, "Cloud computing", *Commun. ACM*, vol. 51, no. 7, pp. 9–11, Jul. 2008. DOI: 10.1145/1364782.1364786.
[59] M. Armbrust *et al.*, "A view of cloud computing", *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010. DOI: 10.1145/1721654.1721672.
[60] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things", in *Proc. of 1st Ed. MCC Workshop Mobile Cloud Comput.*, *MCC'12*, 2012, pp. 13–16. DOI: 10.1145/2342509.2342513.
[61] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues", in *Proc. of 2015 Workshop Mobile Big Data*, 2015, pp. 37–42. DOI: 10.1145/2757384.2757397.
[62] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing", in *Proc. of 2015 IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, 2015, pp. 1202–1207. DOI: 10.1109/INM.2015.7140467.
[63] L. Wang *et al.*, "Cloud computing: A perspective study", *New Gener. Comput.*, vol. 28, no. 2, pp. 137–146, 2010. DOI: 10.1007/s00354-008-0081-5.
[64] Computer chips inside cars, Vintage Computer Chip Collectibles, Memorabilia & Jewelry, CHIPS ETC. [Online]. Available: https://www.chipsetc.com/computer-chips-inside-the-car.html
[65] J. Koscs, "Anti-lock-Brakes: Who was really first?", Hagerty, 2013. [Online]. Available: https://www.hagerty.com/media/archived/antilock-brakes/
[66] Y. Zhang and G. Cao, "V-PADA: Vehicle-platoon-aware data access in VANETs", *IEEE Trans. Veh. Technol.*, vol. 60, no. 5, pp. 2326–2339, Jun. 2011. DOI: 10.1109/TVT.2011.2148202.
[67] U. Lee, E. Magistretti, M. Gerla, P. Bellavista, and A. Corradi, "Dissemination and harvesting of urban data using vehicular sensing platforms", *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 882–901, Feb. 2009. DOI: 10.1109/TVT.2008.928899.
[68] Y. Zhang, J. Zhao, and G. Cao, "Service scheduling of vehicle-roadside data access", *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 83–96, 2010. DOI: 10.1007/s11036-009-0170-9.
[69] H. Zhang, Q. Zhang, and X. Du, "Toward vehicle-assisted cloud computing for smartphones", *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5610–5618, Dec. 2015. DOI: 10.1109/TVT.2015.2480004.
[70] S. Olariu, T. Hristov, and G. Yan, "The next paradigm shift: From vehicular networks to vehicular clouds", in *Mobile Ad Hoc Networking*. Wiley-IEEE Press, 2013, pp. 645–700. DOI: 10.1002/9781118511305.ch19.
[71] R. Hussain, F. Abbas, J. Son, and H. Oh, "TIaaS: Secure cloud-assisted traffic information dissemination in vehicular Ad Hoc networks", in *Proc. of 2013 13th IEEE/ACM Int. Symp. Cluster, Cloud, Grid Comput.*, 2013, pp. 178–179. DOI: 10.1109/CCGrid.2013.38.
[72] M. Gerla, W. Jui-Ting, and G. Pau, "Pics-on-wheels: Photo surveillance in the vehicular cloud", in *Proc. of 2013 Int. Conf. Comput. Netw. Commun. (ICNC)*, 2013, pp. 1123–1127. DOI: 10.1109/ICCNC.2013.6504250.
[73] 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. of 2013 IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, 2013, pp. 439–444. DOI: 10.1109/CloudCom.2013.64.
[74] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985. DOI: 10.1109/TIT.1985.1057074.
[75] V. S. Miller, "Use of elliptic curves in cryptography", in *Advances in Cryptology — CRYPTO'85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science*, vol. 218. Springer, Berlin, Heidelberg, 1986, pp. 417–426. DOI: 10.1007/3-540-39799-X_31.
[76] F. Ahmad, M. Kazim, and A. Adnane, "Vehicular cloud networks: Architecture and security", in *Guide to Security Assurance for Cloud Computing. Computer Communications and Networks*. Springer, Cham, 2015, pp. 571–576. DOI: 10.1007/978-3-319-25988-8_12.
[77] Y. Park, C. Sur, and K.-H. Rhee, "Pseudonymous authentication for secure V2I services in cloud-based vehicular networks", *J. Ambient Intell. Humanized Comput.*, vol. 7, no. 5, pp. 661–671, 2016. DOI: 10.1007/s12652-015-0309-4.
[78] 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, Oct. 2016. DOI: 10.1109/TVT.2016.2541862.
[79] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems", in *Advances in Cryptology — CRYPTO 2000. CRYPTO 2000. Lecture Notes in Computer Science*, vol. 1880. Springer, Berlin, Heidelberg, 2000, pp. 147–165. DOI: 10.1007/3-540-44598-6_9.
[80] W. Wei, R. Yang, H. Gu, W. Zhao, C. Chen, and S. Wan, "Multi-objective optimization for resource allocation in vehicular cloud computing networks", *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, Aug. 2021. DOI: 10.1109/TITS.2021.3091321.
[81] K. Tan, D. Bremner, J. Le Kernec, L. Zhang, and M. Imran, "Machine learning in vehicular networking: An overview", *Digital Communications and Networks*, vol. 8, no. 1, pp. 18–24, Feb. 2022. DOI: 10.1016/j.dcan.2021.10.007.