Internet of Vehicles (IoV): A Survey of Challenges and Solutions

Jawaher Abdulwahab Fadhil
Department of Computer Science,
College of Science,
University of Duhok,
Duhok, Kurdistan Region, Iraq
jawaher.fadhil@uod.ac

Qusay Idrees Sarhan
Department of Computer Science,
College of Science,
University of Duhok,
Duhok, Kurdistan Region, Iraq
qusay.sarhan@uod.ac

***Abstract*—The technological revolution of the Internet of Things (IoT) increased the number of objects (e.g., vehicles) connected to the Internet, making our lives easier, safer, and smarter. Putting IoT objects on the wheel has created a new technology called the Internet of Vehicle (IoV). The massive progress in communication and computing concepts brought the IoV to real implementation. The IoV is the advanced version of Vehicular Ad hoc Network (VANET), mainly designed to provide safe driving. Although the number of vehicles connected to the IoV keeps growing, there are various challenges and opportunities of the IoV technology that are still not clear. In this paper, several research papers related to the IoV were examined to identify and categorize the existing challenges of implementing and employing IoV in urban cities. Furthermore, this work outlines the IoV technical limitations that must be addressed. Moreover, various existing and future solutions that tackle the identified challenges were briefly discussed.**

I. INTRODUCTION

Urban countries suffer from traffic jams and rising road accidents due to the excessive growth of vehicle numbers. In 2001, the VANET was introduced to provide a safe and comfortable driving depending on Mobile Ad hoc Network (MANET) concept. In the VANET, every vehicle is considered as a mobile node and connects with other vehicles wirelessly using Vehicle to Vehicle (V2V) and Vehicle to Roadside (V2R) communications [1]. However, the implementation of the VANET network has become idle for more than ten years because of the complex structure of modern cities and many problems in the VANET network, such as limited coverage, short-live connectivity (if any vehicle loses the connection, another vehicle will connect immediately to the network), and unstable mobile network [2]. In general, the vast revolution in the IoT (a system that enables objects such as sensors and actuators to communicate and talk with each other without human intervention to achieve a common goal) helped to reduce traffic accidents by embedding some IoT objects in vehicles; and this created the IoV concept [3]. The IoV allows vehicles to interact with drivers, other vehicles, environments, and road objects via different wireless networks. Vehicle connection with other infrastructures such as buildings, lights, stations, etc., is called Vehicle to Infrastructure (V2I) connection, while connecting vehicles with other vehicle systems are called V2V connection. The combination of both connection types V2I and V2V is known as Vehicle to Everything (V2X) connection.

Basically, the IoV architecture consists of four main layers: environment sensing, network, computing, and application layers [4]. The environment sensing layer is responsible for gathering data from vehicle surrounding environments such as objects locations, road conditions, and driving habits via Radio Frequency Identification Card (RFID) and sensors embedded inside vehicles. The network layer is responsible for providing all required connection types such as short-range communication (e.g., Zigbee, Bluetooth, and Wi-Fi) or cellular network (e.g., WiMAX or 4G/LTE) between vehicle environment objects and its connection to the cloud. The computing layer is responsible for the process, store, and analysis of the collected data that is needed for providing safety, convenience, risk situation awareness, and efficiency [5]. Finally, the application layer offers two types of services, open services, and closed services. The open services refer to online applications offered by the Internet providers and third-party service providers (e.g., real-time traffic services and online video stream). In contrast, the closed services refer to a specific IoV application (e.g., control panel and traffic instructions) [6].

Connected vehicles within the IoV environment (the combination of road conditions and heterogeneous network connections) are considered intelligent vehicles with a complex internal software platform. The software platform is utilized to manage and control vehicle systems depending on the huge number of data collected from connected objects and information received from the Internet. Converting vehicles from mobile nodes in the VANET to intelligent vehicles with various connection capabilities encouraged many car manufacture companies such as BMW, Toyota, Ford, etc. to start manufacturing their intelligent car and also created high competition between software companies such as Google, Hawaii, Apple, etc. to produce smart IoV applications [7]. The IoV system mainly intended to satisfy the modern Intelligent Transportation Systems (ITS) goals, improve traffic monitoring, energy management, comfort driving, prevent road accidents, and secure vehicular data transmission. Although the recent years showed high progress in the IoV technologies, but still not fully explored, the actual implementation of such systems brought a lot of challenges and opportunities. Currently, several issues need to be addressed in such systems, for example, adapting with vehicles' dynamic topology, dealing with heterogeneous network connections, achieving large scale coverage, and exchanging data securely [8]. However, this survey paper identifies the common challenges of the IoV design, implementation problems, and discusses existing and possible future solutions to tackle the identified challenges.

The rest of this paper is organized as follows: In Section II, the most relevant works are briefly presented.

978-1-7281-8855-3/20/$31.00 ©2020 IEEE

Section III presents different challenges posed by the IoV alongside various possible solutions. Finally, Section IV presents the conclusion of this study with some possible future works.

II. Related Works

In this section, the most relevant studies for this work have been briefly presented. The authors in [9] reviewed the ITS fundamentals required to achieve efficient traffic management between internet-connected vehicles. They also presented the challenges of implementing the ITS on the IoV to gain a safe road with less traffic congestion. They discussed several problems and solutions in the ITS areas, such as broadcasting emergency messages, driving techniques, and communication systems. However, the limited coverage area, message accuracy, and secure communication problems have not been discussed. The authors in [10] have surveyed both technical and non-technical challenges faced by autonomous car manufacturing in terms of implementation and design. Furthermore, they presented solutions related to autonomous car technologies containing its applications and design. However, the authors did not explain using fifth-generation (5G) technologies features in the IoV to solve various problems. The authors in [11] introduced the major parts of the vehicular network structure and discussed its features. Also, they presented an overview of ITS organizations, communication protocols, and programs in various countries, especially in the USA and Japan. In addition, they provided a survey about vehicular network applications, requirements, a number of vehicular network implementation challenges, and discussed possible solutions. However, they did not focus on the role of decentralized cloud solutions and big data opportunities in the IoV area. The authors in [12] reviewed the history of the V2X by studying the old communication types, such as dedicated short-range communications (DSRC), and its development to current status. Also, they provided a comparison between using cellular V2X and 802.11V2X communications; the advantages and disadvantages of each type were highlighted considering the vehicles high mobility behavior and exchanging data in a large scale environment. Challenges related to big data and edge cloud were discussed to create better IoV applications in the future. In contrast, such applications' implementation issues have not been presented, such as the absence of a global application, difficulties of using, and delay issues. The authors in [13] presented a background on vehicular network design and explained motivations toward the IoV improvement depending on three factors: road safety, traffic management, and reliable marketing for the vehicular network. The heterogeneous communications mediums and different IoV layers architecture have also been discussed. Moreover, a brief comparison between the VANET and the IoV has been given. The authors described the IoV enhancement challenges and future aspects requirements in cloud, applications, and network mediums without discussing the existing solutions in the IoV environment. The authors in [14] surveyed the decentralized architecture problems in IoV manufacturing. They examined some open research issues related to the physical and data layers, such as utilizing heterogeneous communication mediums and protocols with various software applications, without discussing the possible technologies to solve these issues in the future. The authors in [15] explained the basics of IoV structure, different IoV architecture layers. Then, they presented the difference between the IoV and the VANET based on a number of parameters such as data size, cloud computing, and range of usage. Besides, they provided a classification of the IoV and the VANET applications in various domains. In addition, they discussed several security aspects in intelligent transmission systems, including existing types of attacks and proposed solutions for each type. However, the authors focused on the aspects based on IoV security only, while other aspects of IoV problems were not addressed.

After examining the most related articles to this survey, it is notable that previous articles highlighted different challenges faced by the IoV technologies without mentioning how to overcome these challenges; a few of them described some solutions and requirements but in a limited way. In contrast, this survey paper addresses the most problems and challenges in the IoV environment comprehensively and discusses the existing and future solutions for each problem.

III. Challenges and Solutions

A. Limited network coverage area

Generally, VANET vehicles collaborate with each other to broadcast emergency signals; vehicles work as service providers and publishers as well [2]. For example, if a vehicle detects an accident, it will notify and inform the surrounding vehicles about the detected accident [16]. Thus, they will continue broadcasting the detected accident to each one and the approaching vehicles. Usually, vehicles share their resources with each other via Vehicular Cloud (VC) using a fixed infrastructure or a cellular network. However, a vehicle cannot publish its request with other vehicles if they are out of the network range. The limited coverage area of fixed Roadside Units (RSUs) is not efficient for VC services due to its mobility in different areas [17]. One of the suggested solutions is to use mobile brokers as a service provider in the VANET environment instead of depending on fixed cloud servers. Each broker stores information and packages of previous vehicle requests. For example, a public bus can act as a mobile broker because it travels in a known path covering a large area of the city [18]. When a request message is sent to the public bus (broker) to find the best match package from the nearest vehicles, the bus will send the service provider ID (vehicle ID) to the requested vehicle to help it to connect with each other and get the required services. If a broker does not find the match package, the request will be forwarded to other closer buses (brokers), if found or to the RSU. In case the matched package has not been found, the vehicle request will be canceled [19].

B. Security issues in the IoV communications

Fog cloud-based IoV is the middle ground between a smart vehicle and a cloud server. It enables vehicles to gather and process data locally and respond to traffic accidents quickly instead of depending on the cloud server [20]. For example, many vehicles within the same area can provide

resources and make decisions quickly for any vehicle request in the same area without sending the request to the cloud and waiting for a response to be sent back. High reliance on wireless communication in the IoV for traffic flow management makes it more vulnerable to various possible attacks such as session key leakage, replay, and data disclosure [21]. However, the common approaches to overcome security issues are:

- Authentication and key management process: Using authentication and key management process between various entities (e.g., vehicles and RSUs) with fog servers. Also, between fog servers and the cloud server such as Diffie-Hellman (DH) key exchange, Public Key Infrastructure (PKI), etc. this will provide more effective communication in the IoV deployment [22].
- Encrypted data/communication: Protect the electronic data (e.g., vehicle user's identity) produced by edge devices while transmitting between fog and cloud; this can be implemented via encryption techniques such as Data Encryption Standard (DES) algorithm and Advanced Encryption Standard (AES) algorithm. The DES algorithm is not suitable for secure sensitive data because the 64-bit key size can be guessed by attackers [23]. Therefore, the ASE is commonly used in fog environments for secure communication because its key size is 256 -bit and cannot be breakable.
- Regular network monitoring: Fog systems need periodic resource monitoring in the network to detect any suspicious function and eliminate it before any damaging activity occurs. Network scanning mechanisms can be done in different manners: static, dynamic, or both. Usually, a large network scan utilizes antivirus, firewalls, etc. to catch any suspicious package depending on network policy and predefined rules [24]. However, fog environments need to implement a new tool and mechanisms for efficient network resource monitoring.
- Wireless security protocols: Many IoT devices are connected to the fog environment and transmit sensitive information wirelessly via RFID, mobile phone, wireless camera, and so on. Achieving secure wireless communication is needed to protect devices' data against attackers (e.g., Sybil attacks) and unauthorized access [25]. For instance, the unauthorized user can access the network from the same station and prevents authorized users from doing some activities by downloading unwanted applications to the network. Employing wireless security protocols such as Wi-Fi Protected Access (WPA) and its versions, including WPA2 and WPA3, supported with the AES are robust solutions in fog environments for secure data transmission [26].

C. *Employ edge computing capabilities in a vehicular environment*

Mobile Edge Computing (MEC) is an approach that establishes individual cloud computing capabilities at the edge point of the network, such as the RSU, central offices, other vehicles, and Base Station (BS) [27]. The MEC helps cars to exceed critical environment situations by collecting and analyzing other vehicle behaviors, weather conditions, and road infrastructure info in real-time without accessing the central cloud [28]. A universal MEC framework is needed to employ edge computing capabilities in a vehicular environment that supports multi-access networks (e.g., LET, millimeter-wave, and IEEE802.11p) and different application types considering the high mobility of vehicles.

D. *Workload on edge applications and job scheduling congestion*

A large number of Artificial Intelligence (AI) and Machine Learning (ML) applications need real-time computing capabilities and resource sharing among network nodes in vehicular environments to improve convenience and safety requirements. This increases job scheduling overload and decreases edge computation capability [29]. This problem can be addressed by decentralizing the MEC into two frameworks. The first one is a decentralized framework called Autonomous Vehicular Edge (AVE); this version of vehicular computing is used to achieve computing capability on neighbor vehicles (V2V) by detecting the nearest available resources based on the surrounding vehicle's location without using any infrastructure such as the RSU or the BS [30]. The second one is called Hybrid Vehicular Edge (HVE); this framework performs online computing capability using the V2V and the V2I connection via a multi-access network. In other words, job scheduling and obtaining accessible resources are achieved online with a minimum waiting time [31].

E. *Centralized cloud and data storage servers*

Currently, many smart vehicles communicate with each other and try to access the cloud frequently. Therefore, using a central cloud server for traffic management between billions of nodes and huge data storage is inefficient for the IoV. Once the server crashes, it may destroy the whole system connection [32]. Blockchain is a list of growly recorded information called blocks; each block has connected nodes information and links to previous and next blocks [33]. For instance, various nodes (vehicles, RSUs, etc.) are connected to separate servers; each server can record nodes data individually as sub-blocks and connected to the main cloud server. As a result, blockchains will reduce communication delays, increase network security, provide massive data storage, and improve overall transportation [34]. Blockchain is the most robust technology to solve centralized organization problems in the IoV, especially in vehicular networks, as it allows for real-time collecting, handling, and storing vehicle information in a distributed manner [35]. In addition, it records transactions between two nodes securely.

F. *Applying In-Vehicle Information (IVI) management systems in autonomous vehicles*

The IVI can be described as a combination of hardware devices and software applications that provide safety instructions and entertainment (video/audio) interfaces for drivers. Hardware devices include sensors, microcontrollers, and actuators controlled via software applications using Bluetooth or Wi-Fi connections [36]. Users can enjoy controlling the whole system using a touch screen, voice command, etc. [37]. For instance, the driver can use a specific application that is already in his/her smartphone (e.g., Apple CarPlay and Android Auto) to display a particular location, call someone, play selected music, etc. by using voice commands while he/she is driving [38]. There are some problems in current IVI systems, including (1) The absence

of a standard system for connecting various IVI devices. Each company has its own application, which is not suitable for IVI systems manufactured by other companies [39]. (2) They need a complex CPU structure to involve different communication interfaces for all IVI system devices because the existing IVI systems do not support all interface communication types in various devices. (3) Limited management techniques are used in the current IVI systems [40], preventing the user from making changes by adding or deleting some devices to/from the installed system.

G. *Providing a good Quality of Service (QoS) in the IoV environment*

The QoS is a set of technologies used to measure network performance, such as error rate, bandwidth, and latency, to achieve a better end-to-end delivery service. Many sensitive data are exchanged wirelessly in the IoV environment that needs efficient QoS to reach the end device with minimum delay and jitter [41], especially multimedia applications (e.g., voice applications and video streaming) that lead to massive load on the networks due to the large numbers of connected vehicles with high mobility behavior and limited bandwidth [37]. For instance, in traffic management systems, real-time traffic data such as voice/video messages need to reach its destination at a certain time in order to take suitable action; otherwise, it will be ineffective and cause traffic problems [42]. The IoV needs to optimize QoS mechanisms that can adapt to different network conditions, particularly when the vehicle joins another network coverage, it will lose the service provided by the previous network connection [43]. This can be done by controlling several aspects to satisfy QoS requirements, such as (1) Media Access Control (MAC) protocol to select the significant time-sensitive package to be transmitted first via channel over other packages. (2) Routing control to achieve minimum delay rate decreases routing floods and solves the connectivity failure problem by providing a multipath routing mechanism [44]. (3) Admission control addresses traffic congestion by accepting/rejecting real-time sessions based on bandwidth accessibility [45]. Some researchers propose to hold routes for time-sensitive traffic to enhance the QoS that satisfies the IoV users' requirements, which is still challenging.

H. *Telematics Service Provider (TSP) in Intelligent and Connected Vehicles (ICVs)*

The TSP is the cloud platform that allows the ICVs to access the Internet and get information from third-party services for good driving performance [46]. Most ICVs come up with a telematics device (e.g., T-Box) connected to the TSP cloud and smart devices (e.g., mobile and tablets) through cellular networks (e.g., 3G and 4G) to provide services. For instance, the Toyota Aqua intelligent car is supplied with many intelligent systems such as intelligent clearance sonar that enhance auto parking control, door control system, and emergency brake control [47]. Vehicle information collected from the T-Box fitted in it and sent to the TSP cloud to get a driving service (e.g., traffic emergency message). Applying telematics services in intelligent vehicles face many challenges compared with traditional vehicles as follows:

- Misuse of the TSP services: Most telematics services come with complex applications that are difficult for the user, resulting in the lost of the provided service advantages [48]. However, to overcome this problem, the TSP service must provide control instructions to the car users, such as providing applications with Graphical User Interface (GUI) or voice commands that guide users to reach the required service.
- Weak authentication: Using simple authentication mechanisms for fast cloud service connectivity in the ICVs makes the system insecure against hackers. That is why robust authentication mechanisms are demanded in the TSP clouds [49]. For example, preventing users from changing sensitive user information such as IP address, phone number, and password without receiving a conforming message from the user.
- Battery life and storage limitation: Driving with low power may lose connection with the TSP cloud [46]. The TSP should consider two factors in the ICVs: battery life and data storage in the vehicle to address this challenge.
- Vulnerable third-party cloud platforms: Providing the TSP from third-party cloud platforms poses security problems that can lead to loss of user's life if this cloud platform is utilized by hackers [50]. Thus, data encryption and secure communication protocols are needed.

I. *Establish well-connected services in Vehicle-to-IoT (V2IoT)*

To receive emergency messages efficiently in the IoV, it is necessary to enhance various communication types (V2X) with different objects. The V2X can increase its connection feature to other objects and various IoT devices (e.g., smartphones and sensors) using Narrowband-IoT (NB-IoT) connection [51]. The NB-IoT is a wireless (radio) technology designed especially for Machine to Machine (M2M) communication. The NB-IoT is sufficient for devices with low bandwidth and low battery consumption [52]. However, V2IoT communications have some limitations, such as (1) The NB-IoT covers a limited area compared to other cellular networks such as the LTE [36]. (2) The NB-IoT does not support direct communication between devices, Device-to-Device (D2D), compared to other communication types (e.g., Wi-Fi) [53].

J. *Utilizing 5G technology in the IoV*

5G technology is the latest generation of cellular networks; this technology overcomes the limitations of previous cellular networks generation (1G-to-4G) with many advantages [54]. In the IoV, all components are communicated together in different scenarios depending on the network infrastructure's wireless network. Vehicles need to keep a connection with other components and environments continuously with large coverage [55]. 5G technology is an excellent choice to implement such communications scenarios; it permits all network components to communicate with everything reliably and securely. It is expected that the new services offered by the

5G networks such as beamforming, Multiple Input Multiple Outputs (MIMO), and network slicing will fulfill the ITS requirements in the future [56]. The 5G tackles the most existing problems in the 4G technology as listed below:

- Limited spectrum: Limited frequency spectrum used in the 4G (2-8GHz) restricts vast network connectivity. The frequency spectrum used by the 5G is a new band of millimeter-wave from 24-100GHz, which is not utilized by other technologies such as GPS, 4G, and Wi-Fi [57]. This provides a vast connectivity rate with more data transmission.
- Limited device connection: In 5G, a small size of antennas is used due to the high range of frequency spectrum (inverse relationship), hence, allowing for a large number of users to connect to networks at the same time [58]. For instance, 100 antennas can be installed in one panel instead of 8 antennas in the 4G, which increasing connection opportunities for a large number of devices.
- Energy consumption: The wireless signal in the 4G is directionless and separates signals in a large area using a standard antenna. As a result, it increases the energy consumption and interferences, especially if different network users are near to each other. In contrast, the 5G utilizes beamforming signals, which are more density and directional than other signals. Beamforming signals provide many advantages, such as higher intensity, less power consumption, and low interference than other cellular networks [59].
- Ensure efficient traffic services: The 5G uses network slicing technology, which is a network architecture that allows splitting the original network into several independent virtual networks (slice) to fulfill various end-to-end service requirements [56]. For example, splitting the physical network into a V2X slice, IoT slice, and mobile broadband slice. Thus, if any slice is damaged, it will not affect other slice connections. This feature enhances efficient QoS (Reliable and low-latency services) [45].

Despite many advantages of the 5G network, it still poses many challenges, such as the coordination between the MEC servers to choose the appropriate server that achieves processing with a lower latency rate [60], and dealing with high mobility features of vehicles. Hence, the vehicle will be available for a short time within the information/resource hosting range. Another challenge is the overwork offloading of computation-intensive tasks on the edge device resource [28]; the 5G needs to address new end-to-end security mechanisms since each slice is considered as the primary network that gives opportunities to new threats types [54], especially in V2V connection and how to effectively manage network slicing and isolate each side's resources [61].

K. Protect the transmitted data and privacy of vehicle users in VANET

The VANET allows vehicles to organize their network and broadcast messages between each other on the road. The serious issue is to prevent vehicle user's information and data integrity from attacks during the transmission [62]. For example, attacking the traffic information from an adversary and sending a fake message for a vehicle to change its road or parking in a specific place for theft purposes [63]. However, many authentication protocols have been employed in VANETs; one of them is lightweight authentication based on smart card (ASC) protocol for secure vehicular networks [64]. The ASC protocol utilizes low-cost cryptographic methods for users' vehicle authentication and data integrity. However, it still performs poorly against the following attacks:

- Offline identity guessing attack: The attacker can obtain vehicle user IDs from the user ID list.
- Location spoofing attack: The ASC protocol is weak against location spoofing (e.g., sending fake location from an attacker).
- Replay attack: The adversary can impersonate an authorized user without using his/her user ID/smart card by replay attack [19].
- Session-Linking Attack: An adversary can track vehicles and break down a set of sessions belonging to the same vehicle [62].

L. Sybil attack detection in Connected Vehicle Systems (CVS)

One of the most critical threats in the IoV environment is the Sybil attack due to the high mobility behaviors and an open environment. The Sybil attacker can pretend its identity to multiple vehicles to access the central server (CS), and this will harm the interests of the honest vehicle [65]. For example, when a passenger requests a taxi from a smartphone using online car-hailing service applications for iOS/Android designed for request nearby Taxi (e.g., Easy Taxi, Uber app.), the current passenger's location is sent to the CS via the GPS. Sometimes, the application may show multiple fake Taxis locations because different Sybil identities location was uploaded to the CS for the same Taxi [66]. Usually, the CS receives vehicle locations data through the BS and monitors trajectories to provide related traffic services (e.g., navigation service). Sybil attacks can be detected by analyzing vehicle mobility behavior to extract the proper path between different fake paths based on the frequent starting point and the vehicle's destination point [15].

M. Ensuring a secure location sharing in the VANET

Vehicles need to share their geographical location with other neighboring vehicles on the road map to avoid traffic jams, collisions, and enable vehicles to make a proper decision. Generally, location sharing problems can be summarized in three points as listed below:

- Localization Accuracy: Location accuracy plays a severe issue in the vehicular communication area. However,

GPS technology does not fulfill the accuracy requirements in IoV fields [67]. For instance, the GPS signal is affected in a crowded area, and GPS based localization does not consider the vehicle speed, which is very important in vehicular communications.

- Location privacy: Vehicle mobility depends on network information, including speed, car ID, position, and safety instructions. Vehicles' information needs a secure transmission mechanism to prevent all possible attackers [68], which is still a severe challenge in VANETs. For instance, a hijacked vehicle may send wrong information to other connected vehicles about a specific location and force them to stop causing vehicle collisions.
- Location Verification: The absence of a trusted authority in neighbor vehicles is also a big challenge in the IoV environment due to a large number of vehicles, information overload, and lack of security mechanisms in VANETs, which is vulnerable to various kinds of threats (e.g., data suppression and denial of service) [63].

N. Prevent traffic accidents

1) Vehicle speed control

Most of cars' accidents are caused by high-speed driving behavior. Controlling the car speed to stay in the limited range is the best solution to prevent traffic accidents. Many techniques are used to adapt vehicle movement to other vehicle mobility behaviors based on road conditions. Possible techniques for vehicle speed controlling are discussed below with some problems:

- AI systems: AI systems are utilized to automatically control the vehicle speed and warn the driver in case of exceeding the limited speed [36]. This type of system still faces some problems such as bad weather situations and poor lighting, making it difficult to recognize the limit speed indicated on the traffic sign by the ML system installed inside the vehicle [68].
- GPS with GSM/Wi-Fi: The GSM/Wi-Fi is used to enhance the GPS work to get the vehicle position's exact coordinates and control the driving behavior. The GPS will detect the vehicle position on the map, and according to that, the speed value will be sent by the Wi-Fi or GSM to the Engine Control Unit (ECU) embedded in the vehicle within the zoon [67]. However, the GPS may fail to find the vehicle's accurate position due to the poor network connection. Furthermore, relying on GSM as a stand-alone system also has problems, such as the need to pay extra money for communication carriers, limited network coverage, and bad weather conditions.
- RFID: The third approach is using RFID based systems. When the RFID readers in the vehicle pass through the tag fixed on the road sign, the vehicle speed will adjust automatically [69]; the RFID problems were compared to other wireless transmitter systems (e.g., RF modules) are short transmission range and relatively expensive.
- RF Transceiver: It processes the received data by utilizing controllers such as CPU, FPGA, and microcontrollers to adjust the vehicle speed automatically and more accurately [55]. The RF transmitter sends the speed data to the controller unit embedded in the vehicle, the connection between the controller unit and ECU will help to warn the driver and adjust the vehicle speed based on the received data [70].

2) Brake control

Vehicles accidents can also be avoided by controlling the brake system, especially when the driver cannot stop the car physically in the required time. The solution is by using IoT technology. For example, two ultrasonic sensors are fixed in front of the car and a microcontroller for car engine control. When the sensor detects an obstacle depending on reflected waves, the microcontroller automatically controls the engine to slow down the car till stop by changing the braking status [71]. In case of car accident happens, the accident information will store in the cloud; then, with the help of the GPS and GSM modules, the accident location will be sent automatically as an SMS to the particular person (e.g., car owner, closer friend, and hospital) [67].

O. Parking management in smart cities (finding free parking place quickly in crowded cities)

Drivers/users need to adapt to the rapid changes in technologies (e.g., mobile apps and communications) used by smart cities. Currently, parking management is required due to car overpopulation, especially in crowded cities. A smart parking system helps drivers to park efficiently and quickly to reduce vehicular traffic [72]. Smart Vehicle Presence Sensor (SPIV-C) is one of these systems designed for private parking places. This system's main components are a distance sensor, Raspberry pi microcontroller, and Pi v2 camera. All these components are located at the back end of each parking place. The system connected with a mobile application (app displays the occupied, reserved, and free parking place), and monitoring center computer (owner of the private parking) via the cloud. The user sends a parking request to the owner and waits for approving his/her request. When the vehicle enters the parking area, the SPIV-C system will capture the car panel and send the vehicle number to the owner as a text message to indicate the place is occupied and save information in the cloud, in case of a car leaving the system shows that the place is available in the mobile app and informs the owner about a free place based on the car number [73]. The SPIN-V system depends on the captured image for the car panel. The limitations to get fully recognized images are camera resolution, the field of vision, working distance, and camera position.

P. Traffic management in large-scale IoV

In IoV environments, when any traffic event (e.g., accident and traffic jams) happens on the road, vehicles will broadcast the message in real-time to inform other users about the action [74]. Implementing good traffic management systems in large scale IoV environments faces a lot of

challenges due to the rapid development of smart vehicles, heterogeneous IoV systems, and traffic flow. The main challenges are:

- Message accuracy: Uploading accurate messages to the traffic management server about traffic events in order to take the correct action [55].
- Large transmission delay: Communication overhead between various IoV elements, including V2V, V2I, and V2X that need to carry/resend messages, will result in a large delay time, making it very difficult to perform such systems on a large scale [75].
- Intelligent routing decision: How to store, carry and forward traffic messages in real-time between the vehicle and other IoV elements depending on the traffic action type [51].
- Information sharing architecture: Encouraging other vehicles to share the traffic action report by improving technologies used in the ITS, such as cloud computing and connected vehicles integrated with the IoT.

Q. Vehicle Routing Problem (VRP) for charging electric vehicles (EVs)

The VRP is a mathematical programming problem (optimization) to find the optimal routes for a vehicle traveling to reach a certain point (e.g., a gas station) with a minimum total road cost and maximum efficiency [76]. However, the VRP limitations are: (1) EVs need frequent battery-power recharging. EVs cannot work efficiently with low power batteries; hence they need an optimal route for getting recharge batteries. (2) Traveling in the mileage range will affect the EVs' connection reliability. For these reasons, traditional VRP solutions are not suitable for battery-powered EVs [77]. The solution is applying a bilateral decision support platform; unlike VRP, this platform depends on an automated expert system (i.e., fuzzy logic) and communication protocols (e.g., MQTT, DDS, and HTTP) to support both EVs and power systems for bilateral decisions (finding the optimal route for the power grid and EVs as well) in real-time [78].

R. Transmitting big data in IoV

In the modern vehicles network scenarios, massive information is generated and consumed between vehicles and heterogeneous resources (V2X) due to massive-scale connectivity and expanding telematics services (e.g., safety applications, IVI, etc.) [79]. Hence, a tremendous amount of data is required to be stored, processed, and transmitted via various connection types. The challenges for transmitting big data in the IoV are:

- Unstable wireless channel connection: Physical elements such as high buildings and bridges on the road may crash the connection between vehicles (V2V) [41]. Thus, vehicles cannot share their information with other environment objects for processing.
- High mobility: A large number of vehicles are accessing the limited area covered by the roadside infrastructures rapidly and frequently, producing overhead Internet access and overload information will affect the driving behaviors and network performance.
- Various vehicle density: Vehicles move at different speeds depending on driving behavior and traffic conditions. Thus, the data transmitting protocols should fulfill the variable vehicles' density requirements in the road by reducing channel resource consumption [80], especially in fewer density roads. In addition, retrieving certain vehicles' data from the cloud is difficult on crowded roads.
- Information overhead: The problem here is how to select the right vehicles in proper time and location to collect, store, and distribute the data to other connected vehicles to achieve long term network management [81].

Finally, Table 1 presents the summary of all the aforementioned IoV challenges with their proposed solutions.

Table 1. Summary of IoV challenges and solutions

	Aspect	Challenges	Possible solutions
A	Network area	• Limited coverage • Fixed cloud servers	• Mobile brokers as a service provider (e.g., public bus)
B	IoV communications	• Security issues(vulnerable wireless communication for various possible attacks)	• Authentication and key management process between entities • Encrypted data/communication • Regular network monitoring • Wireless security protocols
C	MEC	• Multi-access networks	• Universal MEC framework with different application types
D	Edge applications	• Job scheduling overload	• Decentralizing the MEC(AVE and HVE)
E	Cloud	• Central cloud server	• Blockchain
F	IVI	• Various IVI devices • Different communication interfaces • Limited management techniques	• Standard IVI systems manufacturing with open source applications
G	QoS	• Time-sensitive data delay • Connectivity failure • Limited bandwidth	• Hold routes for time-sensitive traffic • Multipath routing mechanism • Admission control based on bandwidth accessibility
H	TSP	• Misuse of the TSP services • Weak authentication • Battery life and storage limitation • Vulnerable third-party cloud platforms	• Provide control instructions to the car users • Strong authentication mechanisms • Battery life and data storage factors should be considered • Data encryption and secure communication protocols
I	V2IoT connection	• Devices with low bandwidth and low battery consumption	• NB-IoT connection
J	Cellular networks	• Limited frequency spectrum • Limited device connection • Energy consumption and interferences • Traffic services latency	• New band of millimeter-wave • Small size of antennas • Beamforming signals • Network slicing technology
K	Privacy of vehicle users in VANET	• Attacks during the transmission	• Strong authentication protocols

L	Sybil attack	• Sybil attack detection	• Analyzing vehicle mobility behavior
M	Location sharing	• Localization accuracy • Location privacy • Location verification	• Consider the vehicle speed factor • Secure sharing mechanism • Trusted authority in neighbor vehicles
N	Car accidents	• High-speed driving • Driver cannot stop the car physically	• Using IoT technology and AI techniques to Control the car speed and brake system automatically
O	Parking management	• Car overpopulation	• Smart parking system using microcontrollers
P	Traffic management	• Sharing traffic action in real time • Communication overhead	• Encouraging other vehicles to share the traffic action report by improving cloud computing and connected vehicles integrated with the IoT
Q	Charging EVs	• EVs cannot work efficiently with low power batteries • Traveling in the mileage range will affect the EVs' connection	• Bilateral decision support platform
R	Big data	• Unstable wireless channel connection • High mobility • Various vehicles density • Information overhead	• Long term network management

IV. CONCLUSIONS

This survey paper contributes to identify and understand various challenges posed by the IoV technology and the possible solutions addressing the identified challenges. This survey was based on investigating a number of recent related papers to extract the IoV challenges and possible solutions. However, the IoV technology is still not fully implemented and thus needs more reliability and effective solutions to be involved such as big data, AI, security, etc. Therefore, further research on such technologies and their roles in the IoV has to be more examined.

REFERENCES

[1] M. R. GHORI, K. Z. ZAMLI, N. QUOSTHONI, M. HISYAM, AND M. MONTASER, "VEHICULAR AD-HOC NETWORK (VANET): REVIEW," IN 2018 IEEE INTERNATIONAL CONFERENCE ON INNOVATIVE RESEARCH AND DEVELOPMENT, ICIRD 2018, 2018, PP. 1–6.

[2] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: A survey," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 3, pp. 996–1014, 2018

[3] A. Richter, M. O. Löwner, R. Ebendt, and M. Scholz, "Towards an integrated urban development considering novel intelligent transportation systems: Urban Development Considering Novel Transport," *Technol. Forecast. Soc. Change*, vol. 155, p. 119970, Jun. 2020.

[4] F. Yang, J. Li, T. Lei, and S. Wang, "Architecture and key technologies for Internet of Vehicles: a survey," *J. Commun. Inf. Networks*, vol. 2, no. 2, pp. 1–17, Jun. 2017.

[5] K. Liu, X. Xu, M. Chen, B. Liu, L. Wu, and V. C. S. Lee, "A Hierarchical Architecture for the Future Internet of Vehicles," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 41–47, Jul. 2019.

[6] W. Wu, Z. Yang, and K. Li, "Internet of Vehicles and applications," in *Internet of Things: Principles and Paradigms*, Elsevier, 2016, pp. 299–317.

[7] X. Cheng, R. Zhang, and L. Yang, "Wireless Toward the Era of Intelligent Vehicles," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 188–202, Feb. 2019.

[8] W. Zhang and X. Xi, "The innovation and development of Internet of Vehicles," *China Commun.*, vol. 13, no. 5, pp. 122–127, May 2016.

[9] G. Dimitrakopoulos, "Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges," in *2011 11th International Conference on ITS Telecommunications*, 2011, pp. 145–151.

[10] R. Hussain and S. Zeadally, "Autonomous Cars: Research Results, Issues, and Future Challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1275–1313, 2019.

[11] Karagiannis, Georgios, et al. "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions." *IEEE communications surveys & tutorials,* vol. 13, no. 4, pp. 584-616, 2011.

[12] H. Zhou, W. Xu, J. Chen, and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," *Proc. IEEE*, vol. 108, no. 2, pp. 308–323, 2020.

[13] O. Kaiwartya *et al.*, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, no. 4, pp. 5356–5373, 2016.

[14] S. M. Hussain, K. M. Yosof, and S. A. Hussain, "Interoperability Issues in Internet of vehicles- A Survey," in *2018 3rd International Conference on Contemporary Computing and Informatics (IC3I)*, 2018, pp. 257–262.

[15] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, pp. 1-44, Dec. 2019.

[16] Q. Wang, D. Gao, and D. Chen, "Certificate Revocation Schemes in Vehicular Networks: A Survey," *IEEE Access*, vol. 8, pp. 26223–26234, 2020.

[17] R. I. Meneguette, A. Boukerche, and A. H. M. Pimenta, "AVARAC: An Availability-Based Resource Allocation Scheme for Vehicular Cloud," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 10, pp. 3688–3699, Oct. 2019.

[18] C. A. Kerrache, F. Ahmad, Z. Ahmad, N. Lagraa, F. Kurugollu, and N. Benamar, "Towards an Efficient Vehicular Clouds using Mobile Brokers," in 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1–5.

[19] A. Guezzi, A. Lakas, and A. Korichi, "A new approach to manage and disseminate data in Vehicular Ad Hoc Networks," *ACM International Conference Proceeding Series*, 2015, pp. 1-4.

[20] A. Thakur and R. Malekian, "Fog Computing for Detecting Vehicular Congestion, an Internet of Vehicles Based Approach: A Review," *IEEE Intell. Transp. Syst. Mag.*, vol. 11, no. 2, pp. 8–16, 2019.

[21] C. Huang, R. Lu, and K. K. R. Choo, "Vehicular Fog Computing: Architecture, Use Case, and Security and Forensic Challenges," *IEEE Communications Magazine*, vol. 55, no. 11. pp. 105–111, 2017.

[22] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues, and Y. Park, "AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8804–8817, Oct. 2019.

[23] A. Vishwanath, R. Peruri, and J. (Selena) He, "Security in Fog Computing through Encryption," *Int. J. Inf. Technol. Comput. Sci.*, vol. 8, no. 5, pp. 28–36, 2016.

[24] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, p. 19, Dec. 2017.

[25] C. C. Lin, D. J. Deng, and C. C. Yao, "Resource Allocation in Vehicular Cloud Computing Systems with Heterogeneous Vehicles and Roadside Units," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3692–3700, Oct. 2018.

[26] W. Xu, W. Shi, F. Lyu, H. Zhou, N. Cheng, and X. Shen, "Throughput Analysis of Vehicular Internet Access via Roadside WiFi Hotspot," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3980–3991, Apr. 2019.

[27] S.-R. Yang, Y.-J. Su, Y.-Y. Chang, and H.-N. Hung, "Short-Term Traffic Prediction for Edge Computing-Enhanced Autonomous and Connected Cars," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3140–3153, Apr. 2019.

[28] I. Sorkhoh, D. Ebrahimi, R. Atallah, and C. Assi, "Workload Scheduling in Vehicular Networks With Edge Cloud Capabilities," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 8472–8486, Sep. 2019.

[29] F. Dressler, G. S. Pannu, F. Hagenauer, M. Gerla, T. Higuchi, and O. Altintas, "Virtual Edge Computing Using Vehicular Micro Clouds," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 537–541.

[30] A. Mahmood, C. Casetti, C. F. Chiasserini, P. Giaccone, and J. Haerri, "The RICH Prefetching in Edge Caches for In-Order Delivery to Connected Cars," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 4–18, Aug. 2019.

[31] J. Feng, Z. Liu, C. Wu, and Y. Ji, "Mobile Edge Computing for the Internet of Vehicles: Offloading Framework and Job Scheduling," *IEEE Veh. Technol. Mag.*, vol. 14, no. 1, pp. 28–36, Mar. 2019.

[32] F. Ahmad, C. A. Kerrache, F. Kurugollu, and R. Hussain, "Realization of Blockchain in Named Data Networking-Based Internet-of-Vehicles," *IT Prof.*, vol. 21, no. 4, pp. 41–47, Jul. 2019.

[33] H. Chai, S. Leng, M. Zeng, and H. Liang, "A Hierarchical Blockchain Aided Proactive Caching Scheme for Internet of Vehicles," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[34] T. Jiang, H. Fang, and H. Wang, "Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4640–4649, Jun. 2019.

[35] C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, Sep. 2019.

[36] D.-K. Choi, J.-H. Jung, S.-J. Koh, J.-I. Kim, and J. Park, "In-Vehicle Infotainment Management System in Internet-of-Things Networks," in *2019 International Conference on Information Networking (ICOIN)*, 2019, pp. 88–92.

[37] Y. Ni *et al.*, "Toward Reliable and Scalable Internet of Vehicles: Performance Analysis and Resource Management," *Proc. IEEE*, vol. 108, no. 2, pp. 324–340, Feb. 2020.

[38] P. S. A., P. C., and K. M. Prasad, "Analysis of Vehicle Activities and Live Streaming using IOT," in *2019 International Conference on Communication and Signal Processing (ICCSP)*, 2019, pp. 0754–0757.

[39] K.-H. N. Bui and J. J. Jung, "ACO-Based Dynamic Decision Making for Connected Vehicles in IoT System," *IEEE Trans. Ind. Informatics*, vol. 15, no. 10, pp. 5648–5655, Oct. 2019.

[40] R. G. Engoulou, M. Bellaiche, T. Halabi, and S. Pierre, "A Decentralized Reputation Management System for Securing the Internet of Vehicles," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 900–904.

[41] R. Florin, A. Ghazizadeh, P. Ghazizadeh, S. Olariu, and D. C. Marinescu, "Enhancing Reliability and Availability Through Redundancy in Vehicular Clouds," *IEEE Trans. Cloud Comput.*, vol. 7161, pp. 1–14, 2019.

[42] M. Shojafar, N. Cordeschi, and E. Baccarelli, "Energy-Efficient Adaptive Resource Management for Real-Time Vehicular Cloud Services," *IEEE Trans. Cloud Comput.*, vol. 7, no. 1, pp. 196–209, Jan. 2019.

[43] S. A. Hussain, K. M. Yusof, S. M. Hussain, and A. V. Singh, "A Review of Quality of Service Issues in Internet of Vehicles (IoV)," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 2019, pp. 380–383.

[44] K. Z. Ghafoor, L. Kong, D. B. Rawat, E. Hosseini, and A. S. Sadiq, "Quality of Service Aware Routing Protocol in Software-Defined Internet of Vehicles," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2817–2828, Apr. 2019.

[45] D. Raj, "Performance Evaluation of QoS in Marine Vehicle to Infrastructure (V2I) Network," in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2020, pp. 876–878.

[46] M. Qiu, W. Dai, and A. V. Vasilakos, "Loop Parallelism Maximization for Multimedia Data Processing in Mobile Vehicular Clouds," *IEEE Trans. Cloud Comput.*, vol. 7, no. 1, pp. 250–258, Jan. 2019.

[47] N. Tamani, B. Brik, N. Lagraa, and Y. Ghamri-Doudane, "On Link Stability Metric and Fuzzy Quantification for Service Selection in Mobile Vehicular Cloud," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 5, pp. 2050–2062, May 2020.

[48] D. Liu, X. Cao, X. Zhou, and M. Zhang, "Cold Chain Logistics Information Monitoring Platform Based on Internet of Vehicles," in *2019 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS)*, 2019, pp. 348–351.

[49] Y. Li, Q. Luo, J. Liu, H. Guo, and N. Kato, "TSP Security in Intelligent and Connected Vehicles: Challenges and Solutions," *IEEE Wirel. Commun.*, vol. 26, no. 3, pp. 125–131, Jun. 2019.

[50] I. Garcia-Magarino, S. Sendra, R. Lacuesta, and J. Lloret, "Security in Vehicles With IoT by Prioritization Rules, Vehicle Certificates, and Trust Management," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 5927–5934, Aug. 2019.

[51] X. Wang *et al.*, "Optimizing Content Dissemination for Real-Time Traffic Management in Large-Scale Internet of Vehicle Systems," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1093–1105, Feb. 2019.

[52] W. Chen, Y. Chen, X. Chen, and Z. Zheng, "Toward Secure Data Sharing for the IoV: A Quality-Driven Incentive Mechanism with On-Chain and Off-Chain Guarantees," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1625–1640, 2020.

[53] Y. Kim and T.-J. Lee, "V2IoT Communication Systems for Road Safety," *IEEE Wirel. Commun. Lett.*, vol. 8, no. 5, pp. 1460–1463, Oct. 2019.

[54] M. Liwang, J. Wang, Z. Gao, X. Du, and M. Guizani, "Game Theory Based Opportunistic Computation Offloading in Cloud-Enabled IoV," IEEE Access, vol. 7, no. c, pp. 32551–32561, 2019.

[55] M. U. Ghazi, M. A. Khan Khattak, B. Shabir, A. W. Malik, and M. Sher Ramzan, "Emergency Message Dissemination in Vehicular Networks: A Review," IEEE Access, vol. 8, pp. 38606–38621, 2020.

[56] D. Kombate and Wanglina, "The Internet of Vehicles Based on 5G Communications," Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016. pp. 445–448, 2016.

[57] J. Cao et al., "A survey on security aspects for 3GPP 5G networks," IEEE Communications Surveys and Tutorials, vol. 22, no. 1. pp. 170–195, 2020.

[58] M. U. Aftab et al., "A Hybrid Access Control Model with Dynamic COI for Secure Localization of Satellite and IoT-Based Vehicles," IEEE Access, vol. 8, pp. 24196–24208, 2020.

[59] S. K. Tayyaba et al., "5G vehicular network resource management for improving radio access through machine learning," IEEE Access, vol. 8, pp. 6792–6800, 2020.

[60] O. Zhdanenko et al., "Demonstration of Mobile Edge Cloud for 5G Connected Cars," in 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2019, pp. 1–2.

[61] X. Hong, J. Jiao, A. Peng, J. Shi, and C.-X. Wang, "Cost Optimization for On-Demand Content Streaming in IoV Networks With Two Service Tiers," IEEE Internet Things J., vol. 6, no. 1, pp. 38–49, Feb. 2019.

[62] H. Vasudev and D. Das, "An Efficient Authentication and Secure Vehicle-to-Vehicle Communications in an IoV," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, 2019, pp. 1–5.

[63] H. Talat, T. Nomani, M. Mohsin, and S. Sattar, "A Survey on Location Privacy Techniques Deployed in Vehicular Networks," in *2019 16th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2019, pp. 604–613.

[64] C. M. Chen, B. Xiang, Y. Liu, and K. H. Wang, "A Secure Authentication Protocol for Vehicular Ad Hoc Network," *IEEE Access*, vol. 7, no. c, pp. 12047–12057, 2019.

[65] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[66] Z. Yang, K. Zhang, L. Lei, and K. Zheng, "A Novel Classifier Exploiting Mobility Behaviors for Sybil Detection in Connected Vehicle Systems," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2626–2636, Apr. 2019.

[67] J. Cheng *et al.*, "Location Prediction Model Based on the Internet of Vehicles for Assistance to Medical Vehicles," *IEEE Access*, vol. 8, pp. 10754–10767, 2020.

[68] H. Xiong, J. Liu, R. Zhang, X. Zhu, and H. Liu, "An Accurate Vehicle and Road Condition Estimation Algorithm for Vehicle Networking Applications," *IEEE Access*, vol. 7, pp. 17705–17715, 2019.

[69] M. M. Bahgat, "Enhanced IoT-Based Online Access Control System for Vehicles in Truck-Loading Fuels Terminals," in *2019 IEEE 6th International Conference on Industrial Engineering and Applications (ICIEA)*, 2019, pp. 765–769.

[70] M. Rana, "IoT-Based Electric Vehicle State Estimation and Control Algorithms Under Cyber Attacks," *IEEE Internet Things J.*, vol. 7, no. 7, p. 874-881, 2020.

[71] S. Srikanth, S. Dhivya, R. Anisha, and S. Hariharan, "An IOT Approach to Vehicle Accident Detection using Cloud Computing," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 2019, pp. 1009–1011.

[72] C. Li, S. Wang, X. Huang, X. Li, R. Yu, and F. Zhao, "Parked Vehicular Computing for Energy-Efficient Internet of Vehicles: A Contract Theoretic Approach," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6079–6088, Aug. 2019.

[73] D. A. Michel-Torres, L. F. Luque-Vega, E. Lopez-Neri, M. A. Carlos-Mancilla, and L. E. Gonzelez-Jimenez, "IoT based Smart Vehicle Presence Sensor SPIN-V for Smart Parking System," in *2019 14th Annual Conference System of Systems Engineering (SoSE)*, 2019, pp. 236–241.

[74] R. Wang, Z. Xu, X. Zhao, and J. Hu, "V2V-based method for the detection of road traffic congestion," *IET Intell. Transp. Syst.*, vol. 13, no. 5, pp. 880–885, May 2019.
[75] S. S. Shah, M. Ali, A. W. Malik, M. A. Khan, and S. D. Ravana, "vFog: A Vehicle-Assisted Computing Framework for Delay-Sensitive Applications in Smart Cities," *IEEE Access*, vol. 7, no. 8, pp. 34900–34909, 2019.
[76] X. Wang, X. Wei, and L. Wang, "A deep learning based energy-efficient computational offloading method in Internet of vehicles," *China Commun.*, vol. 16, no. 3, pp. 81–91, 2019.
[77] Y. Hu, C. Chen, J. He, B. Yang, and X. Guan, "IoT-Based Proactive Energy Supply Control for Connected Electric Vehicles," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7395–7405, Oct. 2019.
[78] A. O. Hariri, M. El Hariri, T. Youssef, and O. A. Mohammed, "A Bilateral Decision Support Platform for Public Charging of Connected Electric Vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 1, pp. 129–140, Jan. 2019.
[79] F. Kou *et al.*, "Common Semantic Representation Method Based on Object Attention and Adversarial Learning for Cross-Modal Data in IoV," *IEEE Trans. Veh. Technol.*, vol. 68, no. 12, pp. 11588–11598, Dec. 2019.
[80] A. Ahmad *et al.*, "Toward modeling and optimization of features selection in Big Data based social Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 715–726, May 2018.
[81] A. Mahmood, H. Zen, and S. M. S. Hilles, "Big Data and Privacy Issues for Connected Vehicles in Intelligent Transportation Systems," in *Encyclopedia of Big Data Technologies*, Cham: Springer International Publishing, 2019, pp. 196–203.