Computing Paradigms in Emerging Vehicular Environments: A Review

Lion Silva, Naercio Magaia, Breno Sousa, Anna Kobusińska, António Casimiro, Constandinos X. Mavromoustakis, *Senior Member, IEEE*, George Mastorakis, and Victor Hugo C. de Albuquerque, *Senior Member, IEEE*

***Abstract* – Determining how to structure vehicular network environments can be done in various ways. Here, we highlight vehicle networks' evolution from Vehicular Ad-Hoc NETworks (VANET) to the Internet of Vehicles (IoVs), listing their benefits and limitations. We also highlight the reasons to adopt wireless technologies, in particular, IEEE 802.11p and 5G vehicle-to-everything in such networks and as well as the use of paradigms able to store and analyze a vast amount of data to produce intelligence and their applications in vehicular environments. We also correlate the use of each of these paradigms with the desire to meet existing Intelligent Transportation Systems' requirements. The presentation of each paradigm is given from a historical and logical standpoint. In particular, Vehicular Fog Computing completes the gaps that Vehicular Cloud Computing seemed to have, so both are not exclusive from the application point of view. We also emphasize some security issues that are linked to the characteristics of these paradigms and vehicular networks, again verifying that because of what they are, they complement each other, hence sharing problems and limitations. As these networks still have many opportunities to grow, whether conceptual or applicational, we finally remember concepts and technologies that we believe are beneficial and enrich them. Throughout this work, we emphasize the crucial role of these concepts for the well-being of humanity.**

***Index Terms*— Computing paradigm, vehicular networks, Cloud, Fog, Edge, IoV.**

I. Introduction

IN this work, we will introduce some fundamental concepts of computing paradigms and their use in emerging vehicular environments and later analyze those that may be more promising in the near future. Usually, these paradigms have a lot in common in terms of the need for proper functioning, particularly in such environments.

Specifically, an efficient, fast, and integrated network is necessary for different forms of wireless connectivity. We chose to adopt a logical perspective instead of a physical one regarding the paradigms' layers in question.

Regarding vehicular networks, we recall the need to provide safer traffic, and therefore protect human life in such networks that are the future of traffic, whether in large cities, on highways, or in rural areas.

Intelligent Transportation Systems (ITS) is a concept that covers connected vehicle networks, but also any other means that involves the cooperative, efficient, intelligent, safe, and economical transportation of people and goods through the construction of an infrastructure that is integrated with the means of transportation in question. Hence, there is a flow of data that, when transformed into information, allows drivers and managers to make the best decisions in perspective and real-time.

A Vehicular Ad Hoc NETwork (VANET) is a specific type of Mobile Ad Hoc NETwork (MANET) where network nodes (i.e., vehicles) self-organize themselves to provide some simple but essential set of services. Internet of Vehicles (IoV) is a novel vehicular environment with more powerful infrastructural elements (i.e., 4G/5G and Wi-Fi-enable OBUs, Access Points to the Internet, connection to the cloud, among others). In conjunction, these elements bring a novel set of applications and services not only going toward ITS requirements but also to commercial ones, given their openness business and people present their applications to this yet unexplored richer environment.

On the other hand, VANET still has its value as it has been in stable development for as long as 30 years. Its distributed and simple architecture suits very well to safety applications

Manuscript received May 12, 2020; revised July 23, 2020 and September 29, 2020; accepted November, 17 2020. This work is sponsored by FCT through the LASIGE Research Unit, ref. UIDB/00408/2020 and ref. UIDP/00408/2020. It was also supported by the Brazilian National Council for Research and Development (CNPq, Grant #304315/2017-6 and #430274/2018-1) (Corresponding author: Naercio Magaia)

L. Silva, N. Magaia, B. Sousa, and A. Casimiro are with LASIGE, Department of Informatics, Faculty of Sciences, University of Lisbon, Campo Grande, 1749-016 Lisbon, Portugal (emails: lsilva@lasige.di.fc.ul.pt, bfmelo@fc.ul.pt, {ndmagaia, accosta}@ciencias.ulisboa.pt).

A. Kobusińska is with the Institute of Computing Science, Poznań University of Technology, Poland (email: Anna.Kobusinska@cs.put.poznan.pl).

C. X. Mavromoustakis is with Department of Computer Science, University of Nicosia, 46 Makedonitissas Avenue, CY-2417, Nicosia, Cyprus (email: mavromoustakis.c@unic.ac.cy).

G. Mastorakis is with the Department of Management Science and Technology, Hellenic Mediterranean University, Agios Nikolaos, 72100, Crete, Greece (email: gmastorakis@hmu.gr).

V. de Albuquerque is with LAPISCO, Federal Institute of Education, Science and Technology of Ceará, Fortaleza, Fortaleza/CE, Brazil, and with ARMTEC Tecnologia em Robótica, Fortaleza/CE, Brazil (email: victor.albuquerque@ieee.org).

between the nearby vehicles and pedestrians. Besides, it can provide simple, nonetheless informative local-based services to the driver, such as nearby gas stations or traffic warnings in nearer electronic road signs.

Vehicular computing paradigms are an essential evolution of cloud and edge computing in vehicular environments. Using the newest communication technologies, and specific protocol techniques, these two paradigms provide a more robust and efficient network, in which cars can act such as cloud servers whenever the situation permits (i.e., in parking lots, traffic-congested roads), but also act as fog nodes where real-time services can run to the benefit of local drivers, pedestrians, business and citizens (if integrated into an interconnected, smart-sensor-fueled environment called smart city [1]).

Nowadays, security requirements such as confidentiality, integrity, availability, authenticity, authorization and access control, non-repudiation, reliability, and privacy are also crucial in vehicular environments, given the latest cyberattacks wave.

There are also some inherent limitations of self-organized networks, such as lack of cooperation among nodes, which pose additional challenges to integrating computing paradigms.

Zhao et al. 2018 [2] analyze deployable vehicle communication technologies, comparing them based on technical and non-technical aspects, and summarizing their limitations. C. Huang et al. 2017 [3] propose a vehicular fog computing architecture besides presenting some use cases. They also briefly discuss some security challenges and potential solutions.

However, and different from previous work, our contributions are the following:

- We provide a roadmap, starting from a historical and logical point of view, giving a small panorama of the intersection between both subjects, namely computing paradigms and emerging vehicular environments.
- We emphasize key security issues that are linked to the characteristics of computing paradigms and vehicular networks, again verifying that because of what they are, they complement each other and share problems and limitations.
- We present our view and hope of what we would consider reasonable for their materialization in the upcoming years when most commercial applications of the concepts discussed here are practical.

The remainder of this work is as follows: Section II presents a historical and conceptual perspective on vehicular communications. Section III presents emerging vehicular environments. Section IV presents computing paradigms. In Section V, limitations and challenges are presented, and Section VI presents security issues. Section VII presents future directions. Finally, Section VIII presents concluding remarks.

II. Vehicular Communications

Both mobile networks and Wi-Fi are expected to receive new generations in 2020, with 5G for the former and 802.11ax for the latter [4], [5]. While 5G networks are expected to help make a leap in vehicle-to-everything (V2X) communications, another Wi-Fi-based vehicle-to-vehicle (V2V) communication standard, i.e., IEEE 802.11p, has been established since 2004. Both will operate in the 5.9 GHz band. IEEE 802.11p is part of the layers of a broader standard, IEEE 1609, which deals with Dedicated Short-Range Communications (DSRC), and among its objectives is communication between stations and Access Points (APs) in a model where the stations are highly dynamic such as vehicles [6].

The U.S. Federal Communication Commission (FCC), which is the regulator for radio, television, cable, and satellite communications, has decided to separate a 75MHz band within the 5.9 GHz spectrum to be used for V2V and vehicle-to-infrastructure (V2I) communications. The goal was to allow applications that would save lives and promote safety and fluidity in transit [7]. Theoretically, DSRC and IEEE 802.11a are similar, nonetheless the former being a version with less overhead than the latter and operating at 10 MHz of channel width, half the width of the latter.

In 2004, the DSRC radio technology was standardized by IEEE given rise to IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) Standard. In Europe, the equivalent standard is called ITS-G5 and was officially adopted on 17 April 2019 [8].

On the other hand, and competitively, there are the C-V2X networks, which have emerged as an alternative and extend mobile networks' capabilities to meet the needs of communication between vehicles, roadside units (RSUs), and even pedestrians. In these, the most significant proponent is precisely the next-generation of mobile networks (i.e., 5G) [9], [10].

5G networks will resolve a set of challenges proposed by the Mobile and Wireless Communications Enablers for the Twenty-twenty Information Society (METIS). Specifically, most mobile devices have numerous purposes for communicating both with the Internet and with each other, thus requiring low latencies, more reliability, throughput, and more scalable algorithms. Moreover, the International Telecommunications Union (ITU) has defined requirements for this new generation that meet low-latency, in the order of 1 ms, and data transfer rates between 100 Mbps and 1 Gbps, with peaks in 10 Gbps [4].

On the one hand, METIS defined as challenges that the network was extremely fast, reliable, multi-purpose, hence allowing a multitude of connected devices and that it would offer a good experience to mobile users, consequently mitigating most of the current common problems. On the other hand, the ITU defined as challenges that the network could offer low latency and high reliability, allow multimedia services in new areas beyond entertainment, be prepared for IoT, and provide greater adaptability in new applications. Also, it would provide great efficiency in applications that are based on where someone is, beyond those specified previously by METIS. Both METIS and ITU do not aim to present protocols to address these challenges, but only to list them given the human needs and world trends of a particular time.

As previously presented, communications in vehicular

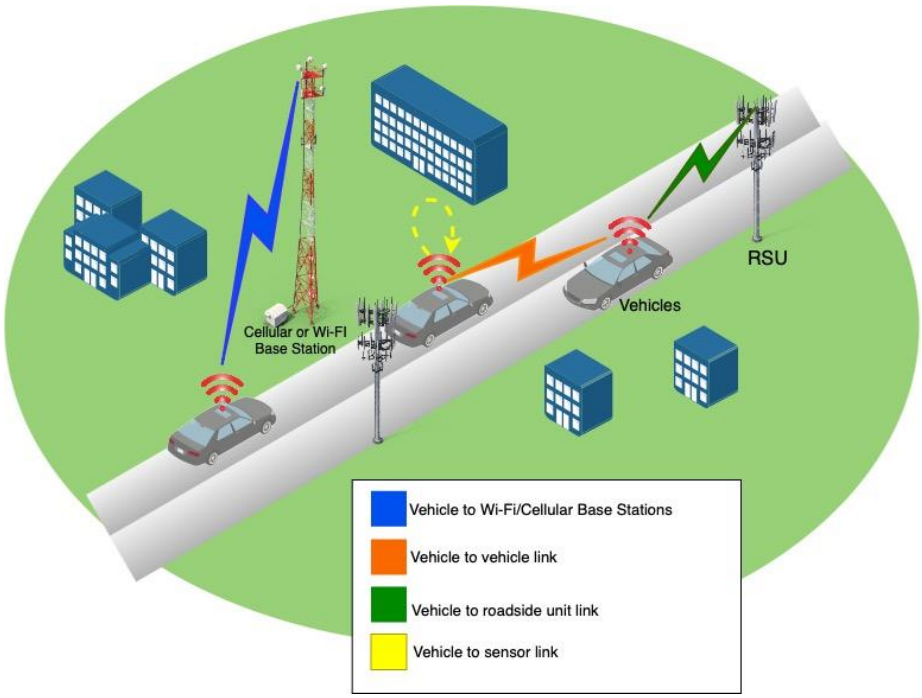


Fig. 1. VANET Architecture

environments can be separated into V2V, V2I, and, ultimately, V2X, where the exchange is done both with the Infrastructure and with other vehicles. If 5G networks make them, we can take into account the following benefits [11], in contrast to IEEE 802.11p:

- *Millimeter-Wave (mmWave)*: there will be high throughput and bandwidth, and this is essential for fast communications between vehicles and things in a constantly changing topology scenario by nature.
- *Non-Orthogonal Multiple Access (NOMA)*: multiple users can share time or frequency resources by multiplexing power or using encoding, where NOMA would give V2X the ability to cancel interference.
- *Multiple Radio Access Technology (Multi-RATS)*: 5G networks could benefit V2I or vehicle-to-network (V2N) communications (i.e., when the vehicle communicates directly to a server or cloud using Cellular Infrastructure) either by increasing network capacity and throughput. Alternatively, by increasing redundancy to increase performance in some remote driving use cases.
- *Antenna design*: using Multiple Input Multiple Output (MIMO) and other techniques and the overall system capacity would be higher and therefore support more V2X activities.
- *In-band Full-Duplex (FD)*: where the throughput would be doubled by using the same band frequency to receive and send data, and
- *Mobile Edge Computing (MEC)*: will enable performing real-time situational awareness, create local maps in high definition, and analyze in real-time the data being exchanged from multiple sources.

Both U.S. and Europe adopt IEEE 802.11p and DSRC as the current acceptable standard for V2I and V2V communications; another part of the industry (the so-called 5G Automotive Association) believes that the future of V2X communications will even be realized by the advantages of 5G networks [12].

According to the 5G Automotive Association, tests have shown that 5G networks can outperform 802.11p networks [13]. From the industry side, the following brands are adopting 5G: Daimler, Ford, Huawei, Intel, Qualcomm, and Samsung. On the other hand, some adopted DSRC: General Motors, NXP, Toyota, Volkswagen, and Volvo [14].

According to both ITU and METIS, 5G networks promise to be ubiquitous once deployed. However, their initial costs may be higher than those of Wi-Fi networks, and the latter, at least, has been around for over ten years [15].

Both technologies have their implementation difficulties, yet they share similar problems as mobile wireless technologies, such as topology dynamics and physical or radio interference from other sources. Nonetheless, the result of adoptions will only be known in the future. Perhaps neither standard will be dominant in the market or as the predominant form of communication in vehicular environments.

III. Emerging Vehicular Environments

In 1994 the first world conference known as World Congress on Intelligent Transport Systems (WCITS) was held in Paris, whose idea was to promote globally what has come to be called by the U.S. Department of Transportation (USDOT), Intelligent Transportation Systems (ITS) [16]. This congress was the first culmination of a history that began in the 19th century with the first traffic light [17]. Today, in full development, it involves millions of devices and sensors in highways, vehicles (e.g., utility, emergency or commercial vehicles, and public

transportation ones), and adjacent structures (traffic lights, CCTV systems, weather stations, event detections).

A. Intelligent Transportation Systems

An Intelligent Transportation Systems (ITS) is defined as advanced information, communication, and electronic technology system that unites users, highways, and means of transportation in order to increase safety, convenience, efficiency, logistics, the productivity of any process involving the transport of people or things [18]. Additionally, it is a concern that these systems reduce the emission of pollutants into the air, and other media aiming at an eco-friendly result.

ITS systems need three general elements: communication, location, and mapping [19], [20]. From this need, these systems are composed of positioning, communication, mapping, network, and sensor technologies. Furthermore, they will have a human-machine interface integrated into vehicles, in particular car navigation systems, so that even basic users are proficient enough, for example, to be able to define a journey, route, or destination [19].

There are six major categories of ITS, namely Advanced Traffic Management Systems, Advanced Travelers Information Systems, Commercial Vehicles Operation, Advanced Public Transportation Systems, Advanced Vehicles Control Systems, and Advanced Rural Transports Systems [18].

Also, there are three main types of ITS architectures: framework ITS architecture, which analyzes and summarizes user needs (functional and practical); mandated ITS architecture, which is the implementation of the previous part, and hence is a set of physical and logical, and communication layers; and service ITS architecture, which, starting from the previous architecture, adds services [21].

Following the development of ITS, vehicles had to communicate with each other in some way. The set of communications, usually wireless, between vehicles is called a vehicular network, and it can be delineated by, among other things, what types of entities communicate with each other. More formally, vehicular networks are wireless networks that are used by vehicles. They are dynamic, heterogeneous, changeable, meeting some requirements of speed, reliability, and integrity to be trustworthy in a non-fixed topology [22].

B. Vehicular Ad-Hoc Networks

The simplest type of vehicular network is only between vehicles and using V2V communications. A more advanced version adds devices fixed on the roads that we travel using V2I communications. The union of these two communications and their technologies forms the so-called Vehicular Ad-Hoc Network (VANET), whose main objective is to optimize traffic and reduce emissions, mostly of gases that pollute the environment [23]. A VANET is a subset of a broader set of networks with mobile nodes, also known as Mobile Ad-Hoc Networks (MANET) [24].

VANETs can still be divided into three categories according to how the communication is being made: (i) WAVE, if the IEEE 802.11p protocol is used and vehicles do not communicate only among themselves, but also between themselves and RSUs, (ii) Ad-Hoc, if the communication is only between the vehicles (and there are no services or connection with the Internet), or (iii) Hybrid if both are implemented concomitantly. RSUs and vehicles are the basic units of a VANET. In this architectural model proposed by the Car 2 Car Communication Consortium (C2C-CC), each vehicle has an On-Board Unit (OBU) and at least one Application Unit (AU). The former deals with the connection between vehicles or between vehicles and RSUs or Hot Spots (to connect to the Internet directly). Meanwhile, the latter serves to realize a set of services/applications and is also connected to the OBU [22]. The OBU does not necessarily have to use Wi-Fi technology as there are other alternatives such as 4G, 5G, WiMAX [24]. RSUs are stationary and linked together in a certain location where they are installed. They will be connected to the Internet forming the infrastructure, where data coming from vehicles and themselves will be the basis for various services aiming at achieving some ITS objectives such as safe driving [24].

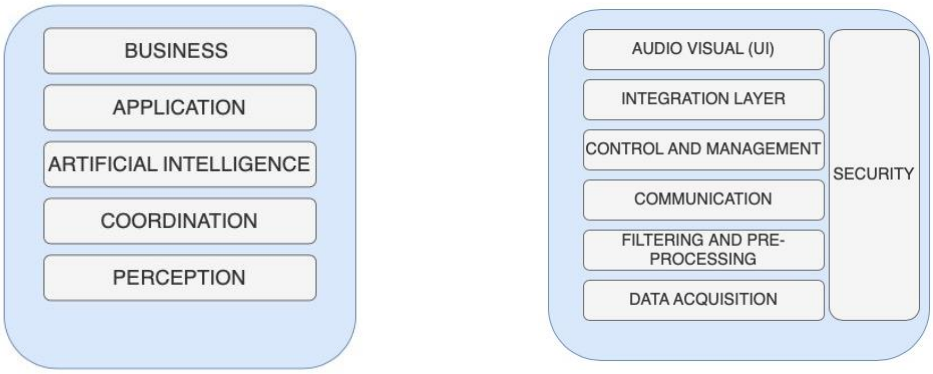
A complete version (see Fig. 1) can consider the separation of RSU functions besides the use of sensors. Therefore, there are four types of communication: V2V, V2I (being the infrastructure of mobile networks, e.g., cellular base stations, or Wi-Fi AP), vehicle-to-sensor (V2S), in the vehicle itself, gathering on-board data from its own operations, and Vehicle-to-RSUs (V2R), where RSUs can be, for example, traffic lights, vehicle-to-pedestrian (V2P), among others [25].

From the infrastructure side, there must be a Trusted Authority (TA) whose job is to manage the entire VANET network by registering RSUs, OBUs, and perhaps vehicle users. This management also includes user and OBU authentication. Ultimately, a TA could act as a substantial Network Intrusion Detection System (NIDS), collecting information on suspicious activities from a particular vehicle or possibly identifying an ongoing attack [26].

Regarding standards organizations, VANETs have been appreciated by IEEE for using 802.11p (and other related protocols), C2C-CC, ETSI, TC ITS, and International Organization for Standardization (ISO). Their main objective is to connect the vehicular network in a continuous and unlimited way with the Continuous Air-interface, Long, and Medium Range (CALM) [22].

ITS problems and challenges are also in VANETs. Specifically,

- In a heterogeneous network with so many nodes, density spikes can happen relatively frequently. In these scenarios, scalability needs to be improved.
- Securing applications and devices that ensure their communications will have to be implemented concurrently with the overall development of VANETs. Security is necessary.
- Quality of Service (QoS) and traffic characterization in VANETs are more difficult because, in addition to the heterogeneity of the protocols of each V2X, applications will also have different QoS requirements.
- Nodes cooperation is based on the fact that each member of the network, i.e., node, is working, sharing, and legitimately receiving information, and is willing to



a) b)

Fig. 2. IoV Architectures. a) 5-layers b) 7-layers

cooperate with other network nodes so that the services are available and reliable to all.

The union of all vehicle-to-something creates the V2X network. However, these networks do not have sufficient global information management power. Usually, they do not analyze, process, or evaluate information collected from vehicles globally [27].

They are thus an intermediate step to what the future vehicular networks will be, that is, the Internet of Vehicles (IoV), which is a specialization of the Internet of Things (IoT), as VANET are of MANET.

C. Internet of Vehicles

Internet of Vehicles (IoV) is defined as a network of the future in which integration between devices, vehicles, and users will be unlimited and universal, overcoming the heterogeneity of systems, services, applications, and devices. It also brings intelligence to the network, i.e., the information is distributed, shared, valued, and meaningful to both the user and vehicular systems, authorities, and service providers [28][29].

Being still a recent idea, different authors have been proposing architectures that differ in certain aspects. For example, O. Kaiwartya et al. [28] proposed an architecture (Fig. 2.a) in five layers:

1) *Business*, the outermost layer, for service sectors to add commercial value to the network.
2) *Application*, the service layer itself, where the intelligence will reside and give the user the feeling of total integration.
3) *Artificial Intelligence*, a second layer of intelligence, but focused on analyzing all information that is being exchanged voluntarily and globally. This is the layer at which computational paradigms will be located.
4) *Coordination*, which is the core that already existed in a VANET, where one defines how and with which technology information will be exchanged (i.e., WAVE, LTE, 5G, among others). This layer, united with Perception, can apply the computing paradigm, such as Fog computing, which will also be discussed later.
5) *Perception*, also already present in VANETs, will deal with sensors, RSUs, personal devices (e.g., AUs). It is at this layer that the information is collected correctly, scanned, and transmitted.

K. Golestan et al. [30] proposed a 7-layers architecture (Fig. 2.b), similar to the previous one, but containing: a data acquisition layer, similar to perception, which collects intra-vehicle, inter-vehicle, and inter-objects data; a filtering and pre-processing layer, which chooses what and to whom to transmit what is collected; a communication layer, which will be responsible for the integration between network technologies (i.e., Wi-Fi, DSRC, LTE, 5G, among others.); a control and management layer, which will serve to control the integration of information traffic and policies applied to the network; a global processing layer that will integrate various types of cloud (i.e., public, private, or enterprise); and finally, the last two layers, which are between the vehicle and the user, with audiovisual interfaces (that is, the user interface layer), and security (that is, security management), vertical, which will cover authentication, privacy, trust, authorization, accounting.

O. Kaiwartya [28] presented a qualitative comparison between IoV and VANETs, showing some perspectives where the former is more advantageous than the latter. For example, reliable Internet services will be available continuously on IoVs meanwhile, on VANETs, whose architecture does not have to be collaborative, Internet service is not available. The processing capacity of the network will be much higher since it is integrated to services in the cloud, as opposed to VANETs, which, in principle, are a network by themselves, not integrated to any Cloud. IoVs will, by default, be integrated between VANETs, Wi-Fi, 5G, and others, making it scalable by splitting and extending services and data transfer across diverse networks reaching somewhere else that one does not reach. Simultaneously, VANETs, because they are not collaborative, have only the local extension of themselves.

Ultimately, IoV can be viewed either as a collection of novel network technologies to provide the layered architecture discussed above. The intelligence is built and somewhat independent of VANET (as if working parallel to it or in its complete absence), or it can use VANET established network for some layers (like coordination). That is because VANET not only is simpler and can take care of such a layer but also already has emergency channels, in which priority messages can be

passed faster.

D. The Importance of Novel Vehicular Environments

Human life is the central element of any technological evolution and revolution. When these happen, suddenly, there is an adjacent enrichment that brings comfort to those who can enjoy them.

When, in the 1980s, the first computers were marketed to families, businesses, and schools, a new way of relating to information began. Later, with the commercial success of the Internet, and especially broadband, along with computers already becoming a common thing, the world was connected and agile. In fact, there were more means by which to expand the Internet concerning the devices that could connect it. With the advent of smartphones and more than ten years after their inception, people are much more quickly and continuously connected. For example, it was estimated that in 2018 there were 3.5 billion people connected to mobile networks [31], [32].

New smart services were being made, such as those of the so-called shared economies, in which a user can make certain goods available to others, being it a host and the intelligent service a platform for the availability of that good. With the addition that, being the interaction made by smartphones, integration services such as GPS, social networks, virtual credit cards could be used all at once, forming a virtual user that could: find the good, know about the owner of that good, and pay for the service associated to its use entirely through the Internet. These types of services that bring together in a virtual user all the information necessary to achieve them were one of the innovations of the last ten years. The next step to be taken is to make connected and intelligent a critical element in the lives of millions of people, i.e., their vehicles.

In general, vehicles still have not received all the connection that in the last 30 years has been established globally by the use of computers and smart devices, and by Wi-Fi, 3G, 4G networks. Connected vehicles, which contain the technology to be considered smart devices, have the potential to increase road safety and driver well-being. For example, in the U.S., in 2017, there was a cost of $433.8 billion related to accidents involving motor vehicles with 40,231 fatalities [33]. In the E.U., in 2016, 25,600 lives were lost in traffic accidents, in addition to 1.4 million people injured [34]. Therefore, road safety is the central element of any process involving the integration of vehicles into an intelligent network.

ETSI ITS defines around 32 use cases to ensure different safety elements between pedestrians, vehicles and other elements [20]. In the basic set of applications, there is, for example, that ITS systems have to enable driving assistance – road hazard warning, with use cases such as emergency electronic brake lights, wrong-way driving warning, traffic condition warning, among others.

These use cases can be more or less divided regarding how they fit for VANET or IoV networks, and that implies both network importance and also differences:

On the one hand, IoV will be better for services that share some intelligence, i.e., higher-level services that use more expensive computation or data storage and manipulation to provide a context about many factors around the network and users. They can be from efficient (less pollutant) carpooling schemes [35] to Artificial Intelligence [36], [37], for example, can be used to provide information about traffic jamming (while texting about it locally with other drivers), or to provide advertisements based on user location and personal preferences, or avoid accidents. AI is one of the critical technologies for IoV applications.

On the other hand, we have VANET that was primarily conceived to inform drivers about harsh conditions or emergencies that could be happening nearby. This includes messages passed by nearby vehicles when facing an unexpected situation where drivers must brake, and the other drivers could not be able to do so as fast as they would if alerted. RSUs can also send messages either to vehicles directly or, after some data computation, to outdoors installed along the road, where they provide almost real-time information.

In short, VANET is essential to road safety situations, and IoV will provide higher-level services, enabling regular programmers to build services too.

The expected benefits of vehicular networks for safer traffic include fewer accidents (mainly fatal ones), more timely responses in their occurrences, less congestion and less pollution, safer social and entertainment dynamism in the use of vehicles, better-informed users of the road, traffic, and route conditions, and more computational power than just the realization of these networks, in the long run, we will be able to know what kind of intelligent services will become.

Therefore, the use of emerging vehicle networks is welcome in the sense that they have the potential to prevent various types of traffic accidents by reducing the costs of loss of human lives and material as never before reduced.

IV. Computing Paradigms

As previously mentioned, the implementation of vehicular networks is planned in several technological aspects depending on the adopted architecture. Mainly, there are two aspects to consider depending on the type of wireless communication, namely 5G networks' V2X or IEEE 802.11p. VANETs were also considered somewhat archaic networks, and consequently, the need to introduce "intelligence" in the network, which motivated the appearance of the IoV concept. There are also other essential aspects to consider, for example, in relation to how heterogeneous we want the network to be, that is, how many different types of services and devices participate in it; and how can we distribute the analysis of the collected data in a way that the most important ones immediately or in a real-time measure, have low latency in their distribution and/or collection or are readily available where they are most needed. It is also necessary to define, with the data that are not of immediate need, where they will be kept, such as the number of times that there was a traffic jam on a certain road during a certain month of the year, and who will process it to make statistics or build relevant information for users, authorities, and service providers.

A paradigm is a specific way of seeing or understanding a

particular thing. In the context of vehicular networks, one way to solve, in part, the problem of data availability where it is most needed, especially when there are real-time requirements, and when the stakeholders are network elements close to the vehicles or their users, is through computing paradigms. Moreover, one way to be able to store and analyze a vast amount of data to produce intelligence and relevant information for a moment after the collection is also through computing paradigms.

A. Cloud computing

According to NIST [38], cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It became common in the literature to use NIST's definition. Nonetheless, it is interesting to note that ten years ago, when cloud computing was in its early days, there were so many definitions that some authors decided to bring them together in the search for the striking and common features [39].

An important feature of cloud computing is that its services and means of provision can be sub-categorized. Thus, the cloud is composed of the characteristics that will concretize its proposal as defined above, and also by how those characteristics that will be used for the cloud to behave in a certain way, defining the service model. Finally, those characteristics will demarcate who is responsible for its management. Depending on the latter, there are three basic models and a hybrid one [40] that unites them:

- Private cloud, where the manager is a private entity, typically a technology company.
- Community cloud, where the manager(es) has(ve) some policy requirements that are shared and involve the use of the cloud, and whether these policies are common concerns of managers and users or even some common mission to achieve.
- Public cloud, where the manager may be a government, academic, or even private entity, but the use of the cloud is open to any user. The purpose can be varied.
- Hybrid cloud, in which the manager(es) mix the previous models, noting that the way they are interconnected is by some technology that still distinguishes each cloud as a distinct entity.

Despite these being the base models, there are others such as the Inter-Cloud [41], [42], and its two main variants: Multi-Cloud and Federation Cloud and Micro-Clouds and Cloudlets, Ad-Hoc Clouds, and Heterogeneous Clouds.

Inter-Cloud allows for different clouds to collaborate in order to ensure greater availability of services for users (e.g., for vehicular networks, monitoring, and vehicle maintenance services) [43] as well as the gain of computational resources [44]. One of the reasons Inter-Cloud is recommended is because while cloud computing providers are concerned with configuring their data centers in different geographic regions, they have a limitation in creating policies that ensure optimal load balancing between different data centers, as well as ensuring optimal QoS [45]. In [43], a framework was developed using business models based on Platform Production Services (PPS), IoT, and Inter-Cloud computing aiming at convenience, efficiency, and safety in Vehicular Networking Applications (VNA). In this framework, for VNA stands out the use of cloud services for scalability of the computing level and an Inter-Cloud architecture that supports telematics applications and scenarios.

Multi-Cloud computing [46], [47] refers to the relation between different service models of Cloud computing (i.e., Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS)), being this motivated by the variety of implementations and administrative domains of Cloud computing.

Federation Clouds [48] are those where a service is offered with shared resources between public and private providers that rationalize the use of their clouds and mutually increase computing power, avoiding service disruption. Implementation is difficult because the best way to define integration rules is still diverse, although efforts in this direction have been made for a long time [49].

As for the component of services that the cloud can offer, three basic types may have sub-categories to the extent that innovation allows [38]:

- IaaS: In the scale of services, this is the "lowest level" offered in the sense that the user hires a subset of computational resources (whole operating systems, storage, processing, and main memory) in which he can operate in any way he wants. He will have no control over the cloud infrastructure itself, nor the entire network.
- PaaS: In the scale of services, this model is intermediate, in which the user no longer has the control he had in IaaS. However, he can have control of some host settings so that applications made in languages and libraries supported by the provider run as desired. These applications can be made, and usually are, by the user.
- SaaS: In the scale of services, this model is the "highest level". In it, the services are made by the provider, and the user buys the right to use them in the cloud but cannot modify the application or any underlying aspect of the infrastructure that runs it.

Other examples of under the "as-a-Service" collection include Backend-as-a-Service (BaaS), Storage-as-a-Service (STaaS), Cooperation-as-a-Service (CaaS), Traffic-Information-as-a-Service (TIaaS), Vehicle-Witnesses-as-a-Service (VWaaS), Mobile-Backend-as-a-Service (MBaaS) [50], Database-as-a-Service (DBaS) (i.e., Relational Cloud) [51], Network-as-a-Service (NaaS) [52], and Function-as-a-Service (FaaS) [53].

In order to implement a cloud architecture in the general case, it will be necessary a collection of data centers providing different kinds of services that can be resumed in storing large amounts of data as well as performing high demanding computation tasks. Also, since the cloud is thought of as a seamless computing resource that a user can use but not exactly possesses, the services are accessed by network infrastructure.

Table 1: VCC vs VEC Comparison

Feature	VCC	VEC (VFC)
Geographic Location	Remote	Near users
Latency Quality	Low	High
Communication	Limited by Network infrastructure when using Cloud	High enough to real-time
Computing Power	Between medium to high	High if achieving fully expected integration
Cost	High (big when using the cloud, also can be bigger than VEC if memory in vehicle for "big tasks" is a must)	Low (granular, vehicle by vehicle built in)
Dynamics	Expected to be somewhat stationary	Ephemerous, and rapidly changing
Applications	- Offloading services - All sort of X-as-a-Service (e.g., NaaS, STaaS, CaaS, among others) - Statistical, machine learning, knowledge-based services	- Real-time applications - Network distribution - Road safety services - Infotainment - Offloading services
Advantages	- Good storage and computing power once acting as a unit (the cloud itself) - Good in traffic jamming situations - Share benefits of general cloud computing, such as serverless computing methods.	- Deployment costs are lower than VCC. - Granularity is higher, since every vehicle can be a Fog node. - Real-Time services possible given proximity to the users
Disadvantages	- Costly to apply. - Better suited only when vehicle is about to stay still for a long time. - Higher latency, therefore, not adequate for urgent, real-time, or high priority applications.	- Lacks agreement to cooperation between different Fog networks - Lacks better suited security protocols given dynamism of network - Lacks convenient wireless protocols for higher throughput, resource hungry applications.

The machines used need to have virtualization technology in such a way a virtual layer can be used to provide transparency of the services as a whole and protection for each individual machine, in which virtualization emulates specific operating systems and configurations for final users.

The services can be distributed between cloud data centers, but, in general, one can view this as a centralized paradigm since all users need to be served from a particular cloud most of the time in a client-server model. As previously stated, the nature of the cloud and services can vary.

Finally, an efficient cloud implementation requires algorithms for energy spending, task distribution, besides efficient revenue maximization, as the complexity of offering such services often does not provide the best way to manage the cloud's resources, lowering both for those who use and offer them.

In this respect, J. Bi et al. [54] and H. Yuan et al. [55] give optimization methods for different parts of the clouds' management process. They, among others, indirectly target the economy in and around cloud computing and directly target resource provisioning because many external cloud services are allocated to its environment.

For the first work, it is the very allocation of heterogeneous resources from virtual machines to Virtualized Cloud Data Centers. In conclusion, several Service Level Agreements are met more cheaply and efficiently. Regarding the second, an algorithm (i.e., Temporal Task Scheduling Algorithm – TTSA) distributes tasks in a Hybrid Cloud environment that unites a Private Cloud (i.e., a restricted resource Cloud), and Public Clouds (i.e., an unrestricted resource Cloud) so that the former is not overloaded, and then manages to decrease the underlying operating costs.

B. Fog computing

Fog computing [56] is defined as a way to extend cloud services to the edge of the network. It is based on the philosophy that data should be processed where it is collected [57], [58].

The edge consists of two sets of devices. The first ones are devices that will consume or send data on the network; however, as users of one or more services made possible by the network itself, without contributing to its infra-structural functioning. End devices can be smartphones, IoT devices, vehicles, sensors, or others, simply having the necessary hardware to connect, and mean something within the service provided by the network. The second set of edge devices are those that are part of the network infrastructure and that intermediate access to services, either by managing the data that passes through them, or by providing access to the services, or also serve as a data storage point.

Fog computing aims at solving problems that arise when the number of devices to access the network is so high that QoS

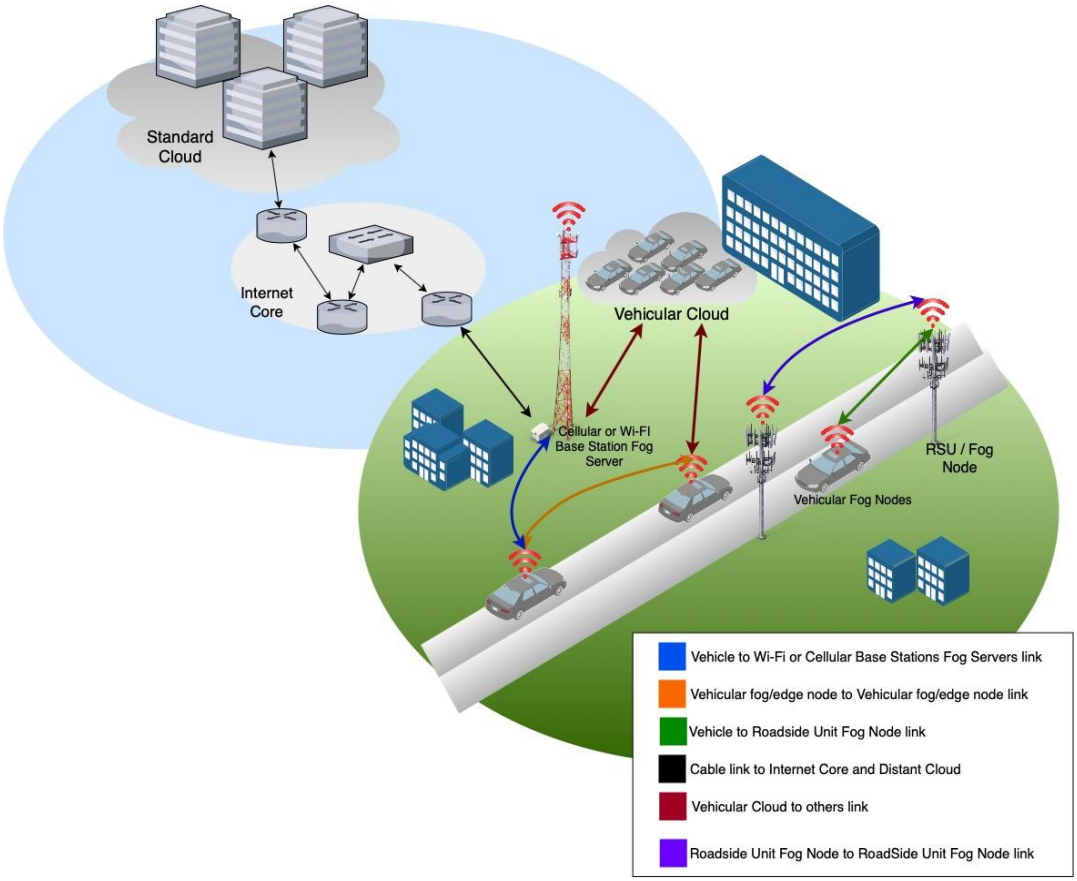


Fig. 3. Interactions between Vehicular Cloud and Fog (or Edge) paradigms

metrics such as latency, response time, among other performance metrics, fall below the minimum defined for the well-being of the user and the requirements of the services provided. Ultimately, it can be a paradigm to extend network scalability, given the innovations to be leveraged with smart devices.

A. Dastjerdi et al. [56] proposed a possible architecture for fog computing consisting of three main layers: cloud, edge devices, and the network between them. Between the cloud and edge devices, there will be a layer of software that enables the infrastructure. This layer does not explicitly deal with end-user services or network protocols but with managers and performance monitors orchestrating the operation of cloud and fog services. In the outermost layer lies the services themselves, that is, the innovations that providers can offer or that will be created by third parties.

According to J. Xu et al. [59], the following tiers should be considered to implement a fog architecture:

- User-Tier: the implementation will be based on diverse types of sensors, smart devices, vehicles using Wi-Fi, Bluetooth, LTE, 5G, or other wireless technologies to communicate between each other and with the Fog-Tier.
- Fog-Tier: the implementation will be based on different nodes, namely switches, routers, access points, and dedicated fog servers.
- Cloud-Tier: the highest tier contains multi-purpose data centers to operate in a fog context for services that are not in real-time.

The User-Tier will be served by real-time services by fog nodes since they were designed mostly for this type of service. Nevertheless, not only services that can build a context awareness from a more prominent view can be built in the Cloud-Tier. The latter will be presented back to the lower tiers in the form of better distribution of fog nodes and fog layer abstraction software, and for the users for a better experience.

The Fog-Tier will distribute data and perform computational offloading so that the services can be experienced both on the location they are being provided or in a decentralized manner, protecting the lower layer from having slow responses and poor QoS.

The Cloud-Tier will be used to gather data that is not immediately used by the User-Tier in a real-time context. Then, some computation can be performed to obtain statistics, AI, and other knowledge-based services, besides other computationally demanding services. Please note that more information can be found in [60].

C. Other computing paradigms

Other paradigms are close to cloud and fog computing. Specifically, edge computing [61], which does not connect to the network, and the infrastructure and service is between end

devices and edge devices. Mobile Cloud Computing (MCC) is similar to cloud computing, although for mobile devices where moderation of use is considered due to limited energy capabilities, and a problem for computing-intensive services. Moreover, Mobile Edge Computing (MEC), which, similarly to fog computing, aims to be between users with mobile devices and the mobile network [62].

Besides these, there is dew Computing [63], [64] that is located at the floor level of the cloud and fog computing environment. It is much more about the microservices concept (in which its computing is vertically distributed) than solely storage/networking. Mist Computing [65] is similar to fog computing but lighter and closer to endpoints than the fog itself. It is done by using microcomputers and microcontrollers. These specialized and near peripherals are the helpful counterpart to more powerful fog nodes. Mist nodes can help IoT devices to have self-awareness and self-organization capacities. Finally, cloudlets [66], [67] are a lighter version of the cloud services and infrastructure. They are put near mobile devices, and the intent is to provide access to the Internet, storage, and somewhat powerful computing. They are usually small datacenters powered with virtualization technologies in such a way mobile devices can offload their computation to them.

D. Computing paradigms in vehicular environments

Here, we revisit the definition of concepts such as fog, cloud, and edge computing in vehicular environments as follows:

- Vehicular Cloud Computing (VCC). VCC [68] is the case where vehicles will be functioning as a cloud, i.e., when together, they form a kind of computational "cluster" with the processing power equivalent to that required for certain "large services", and possibly will be used as temporary storage of large volumes of data. Optionally, there will be Vehicles using Cloud (VuC) [69], where the cloud will be an external entity to the vehicle network, but connected to it, probably far away, from a service provider that does not necessarily own or manage the vehicle network in some way.
- Vehicular Fog Computing (VFC). In a vehicular environment where services, processes, data, policies whose execution time, transmission latency, and availability need to be measured in real-time, so we can restructure each vehicle as a dynamic part of that network by offering computational power for those sets of operations provided within the network in order to decrease the overhead of "large services" or simply eliminate them when it is possible to solve network needs locally [70]. A Fog Vehicular Computing (or Vehicular Using Fog Computing) [71] network will be a vehicular environment whose fog nodes are RSUs, or any other geographically distributed equipment to meet the needs of the VFC without necessarily having any vehicle as a fog node.
- Vehicular Edge Computing (VEC). The term VEC can be seen as a generalization/variant of VFC, just as fog computing can be seen as a variant or implementation of edge computing [72]. Furthermore, as MCC is the paradigm that encompasses VCC, MEC is the paradigm that will encompass VEC (and VFC) [73]. Therefore, we take this perspective only with the difference that edge nodes are vehicles, and then, if edge computing is used, RSUs will be edge nodes.

Table 1 summarizes what is consensual about VCC and VEC paradigms. Please note that some advantages or disadvantages mentioned are simply because of current technological limitations, instead of general architectural faults.

Depending on the infrastructure of each of these types of vehicular networks, we choose to summarize in two figures uniting all these paradigms as we describe them in a way that is in line with the literature. In Fig. 3, we emphasize the global vision. It should be noted that the way services are going to be implemented and distributed should not strictly follow this organization. However, it is expected that the implementations take advantage of the architectures presented. Besides, the expectation that the cloud is distant, and therefore denoted in Fig. 3, is valid since most cities will most probably not have a large computing center from service providers such as Google or Amazon. However, nothing prevents other types of clouds more locally scoped, from intermediating even large service providers or merely solving local storage and data analysis needs.

Other essential aspects are:

- The use of 4G, 5G as well as IEEE 802.11p is critical to achieving the level of ubiquity that METIS ITS standards require.
- Both VCC and VFC would divide the intermediate layers, redirecting the data according to the type of service provided and their priority.
- A VCC does not necessarily need to be connected to the Internet (Fig. 3), but a VuC does.
- An RSU does not need to be a fog server if vehicles are already a distributed fog server or nodes. However, in order to increase the granularity of the network and to guarantee that in specific geographical points there will always be a fog node available, excluding eventual failures, RSUs can pack a server as a minimum computational power and storage that may be considered necessary for the most basic services that the vehicular network offers at that point.
- In principle, the Vehicular Cloud can be used in places of high concentration of parked vehicles for a long time. In such cases, this cloud may eventually serve clients other than those of the enterprise in which they are parked. This will depend on the interest of various involved parties (i.e., users and managers).
- If both paradigms are available, and if vehicles have more than one way to connect wirelessly, it may be interesting to separate the paradigms for each type of connection, such as real-time data passing through 4G, 5G to VFC, and data for later analysis and intelligence building through IEEE 802.11p to Base Stations. Thus, if a group of vehicles is facing congestion that is predicted to last for a long time (e.g., one hour or more), the vehicles may decide to form a cloud while performing fog node

Table 2. VANET characteristics and possible security issues

Characteristic	Security issue
Wireless communication	To properly encrypt data flows, implies a tradeoff between security and overhead.
Dynamic network topology	Fast-changing and transition between entering and leaving nodes will require novel authentication methods and handshake protocols specially design for such networks.
Network size	The lack of standard or global authority across geographic borders could mean privacy concerns and coordination difficulties between VANET networks.
Trustworthy data being exchanged	For the correct functioning of the network, nodes need to be able to trust each other, which implies that data integrity and reliability must be guaranteed.
Infrastructure and OBUs	Both elements can be tampered, although with some difficult because of the constant vigilance to protect RSUs, and the inherent hard task of opening, finding and modify an OBU of a given vehicle.

Table 3. IoV characteristics and possible security issues

Characteristic	Security issue
Dynamic topology	IoVs will have an ever-changing topology in which the verification of entering and leaving nodes needs to be fast and reliable. Also, it should not be extended to any malicious network aggregation where malicious agents could act.
Large scale network	The future integration between nodes, infrastructure, and other devices in IoVs will bring novel security challenges.
Wireless communication	Similarly to VANETs, but also considering real-time communication, any kind of communication jam, even unintentionally, could damage material and human resources.

functions at the same time using different types of wireless communications.

V. Limitations and Challenges

A. Limitations

Up until now, we have described and even discussed some limitations of each of the paradigms as well as the associated vehicular networks. Here, we extend this discussion even further.

In IoVs, the following factors, although necessary for their proper functioning [74], still present some limitations: (i) *interoperability of network architectures*: there is a need for the development of communication protocols to ensure better transmission of a large volume of data as well as interoperability, meeting IoV requirements; (ii) *intelligent routing and route planning*: the constant modifications of the network topology, due to the high vehicles' mobility makes it necessary for IoV to take measures to define routes in the communication layer as well as to ensure that autonomous vehicles are able, for example, to find routes with the shortest distance and lowest cost; (iii) *sensors and AI*: the use of AI can reduce the effort to process data collected by various sensors scattered on highways, and assisting in decision-making; and (iv) *real-time massive data processing*: combining sequential and parallel processing is essential to optimize processing limitations since it is necessary to integrate parallel data acquisition, data processing and Big Data analytics in IoV.

The following possible limitations have been identified in VANETs: RSUs communication, cooperation with other networks, Standards, and complexity and technological infrastructure [24], [25], [75].

Specifically, concerning the first: (i) the number of RSUs available on the road: vehicles need to send and receive data from the network, where the lack of Internet signal (a signal that in this scenario comes from RSUs) will directly influence the communication with the cloud; (ii) limited communication range: in addition to the previous limitation, the communication range is a fundamental requirement due to the nature of vehicles themselves, i.e., they are constantly moving away from the physical positioning of RSUs; (iii) low-quality communication links: data transmission failures may occur due to low signal quality, being necessary to find alternatives for sending and receiving data.

Regarding the second, VANETs are focused on safety, that is, focused on the current traffic situations, not particularly on entertainment (or similar). Therefore, they do not integrate, a priori, the Internet, and reduce costs; the option is to use WAVE or 5G, but not necessarily both. In addition, they do not integrate other types of networks such as IoT, as VANET's data is produced and disseminated by vehicles, RSUs, and Base Stations.

Concerning the third, communication standards already exist in VANETs, and they deal with general aspects such as how a node enters or leaves the network. However, it is thought that it might be better to produce more refined standards for the Cyber-Physical Systems involved, for example, vehicles, motorcycles, buses, ambulances, among others, as we have seen before in the architectural components of an ITS. Besides, having a global coupling standard between VANETs will be necessary as they grow, and different providers and public agents realize that their networks will be meeting geographically.

Relating to the last, one of the factors that make the popularization of VANETs more difficult is that the implementation costs are still high given the interest that people

Table 4. VCC characteristics and possible security issues

Characteristic	Security issue
Virtualization of machines	One of the main benefits of Cloud computing is resource sharing, virtualization, and isolation of the virtual machines (VMs). Problems can occur when the isolation is faulty, and an attacker access other virtual machines or even the host.
Data storage	Security issues can range from physical attacks, where an attacker has access to the Data warehouse through weak cryptographic schemes used to protect the data.
Cloud applications	Without proper isolation and virtualization, the Something-as-a-Service service models can lead to security exploits such as buffer overflows on VM Hosts.
Availability	By natural cause or human interference, the availability in VCC services could suffer in both ways making data inaccessible to the user.

Table 5. VFC characteristics and possible security issues

Characteristic	Security issue
Information exchange between nodes	Nodes' privacy and data integrity need to be guaranteed. Otherwise, issues such as eavesdropping, credential theft, data corruption and tampering can occur leading to undesirable network or service behavior.
Distributed resources	The good functioning of the network could disrupt either by overloading services with spam data or depleting Fog nodes' resources by the use of malicious service.
Nature of the paradigm	VFC relies on wireless communications and resource sharing. Denying Fog nodes access to the VFC disrupts its very purpose and happens either by the stopping new Fog nodes to enter the VFC or by hijacking infrastructural Fog nodes (RSUs).

have in possessing a vehicle with connection capabilities to participate in them. Moreover, an RSU most probably is an expensive device [76]. It is also about a physical structuring of space, with structural changes in cities, highways. So, it is complex both in terms of strategy and management, and interest on the side of public and private agents.

Acceptance, resource management, and suitable technologies are some of the limitations of Vehicular Clouds [77]. Specifically, acceptance is practical and not technical. The owner of a vehicle must have reasons to want to participate in a VCC, as it implies sharing its resources, and there must be a benefit for him to be interested. Commonly, vehicles do not automatically participate in a VCC, nor are they obliged to do so. Then, it is necessary to make choices regarding load balancing, data dissemination, and resource allocation. That is, it is still necessary to deal with algorithms that distribute resources efficiently from an energetic and computational point of view so as not to overload the vehicles. Therefore, the idea is not to generate expenses higher than those required for those who ask for them (in the same way as a Cloud Service Provider would charge for using the cloud, the vehicle owner may also charge). Lastly, VCC networks lack the central element that will make them possible, i.e., a medium or a set of wireless communication means that are fast enough for the massive demand for data traffic that is expected. WAVE or 5G can be used, but network saturation, even for these two types of communication, might be achieved relatively quickly, increasing the cost of implementation and use.

For Vehicular Fog, there are the same questions given above for VCC and besides others, namely network topology and mobility model, and privacy [78], [79]. On the one hand, although in Vehicular Clouds, it is not always necessary to worry about network dynamics, in the case of VFC, it is mandatory. One of the assumptions is that nodes are incredibly dynamic and fast (i.e., they are moving vehicles). The Mobility Model should predict which vehicle enters and exits or which sub-part of the network it is heading to in real-time. Furthermore, currently, there are neither protocols nor ways to integrate this network in the ubiquitous way that one so desires, mainly because VFC is presently a growing topic.

On the other hand, it will be necessary to keep fog nodes private and, at the same time, known on the network. The differentiation of what can be shared and kept secret is still a limitation under study. For example, to mitigate part of the network topology problem, fog nodes could be willing to disclose their location in real-time, and that the network knew the route of any GPRS device they used. However, this possibly constitutes a privacy breach.

It is also necessary to consider Big Data since and as previously stated, the volume of data expected today and in the upcoming years is in the order of zettabytes. Besides, all this data may be used to understand the usage patterns of certain services, the general network behavior, and QoS.

W. Xu et al. [80] describes both topics, i.e., IoV and Big Data, that we highlight below:

- Wireless Condition: it suffers from various blocking elements, such as buildings, other cars, and networks. From the vehicle's perspective, these obstacles seem multiple due to the constant movement factor. Thus, the topology dynamism is a crucial factor. Big Data applications and services will suffer as any other since this is a global scope problem.
- Spectrum resource shortage: Considering an IoV

Table 6. Common attacks and possible solution(s) in vehicular networks

Attack	Description	Possible solution(s) from literature
Malware	Multi-purpose malicious software (e.g. Ransomware)	[139], [140], [141], [142], [143]
OBU Tampering	Any physical OBU alteration in such way the data can be get without authorization	[144], [145]
Spamming and Phishing	Malicious non-authorized or desired message sending across networks and nodes in order to deceive users or entities (vehicles, in this case)	[146]–[148]
Malicious (Rogue) Node	A Node which purpose is solely to deviate the traffic or consume computation/storage resources from the network it is withing.	[149], [150], [151], [152], [153]
(Distributed) Denial of Service	An Attack where a node receives too much requests to certain service ultimately surpassing its computing capabilities to solve them, thus failing to provide the service.	[154], [155], [156], [157], [158], [159], [160]
Masquerading, Impersonation, Sybil	Attacks where the attacker can hide its identity behind either: fake user, legit user or an apparent group of users	[161], [162]
Sniffing, eavesdrop, man-in-the-middle	Attacks, mostly passive, where attacker exploits a vulnerability in communication mediums to break the confidentiality of information (or even its integrity in MitM)	[163]–[165]

implementation, the number of applications that will follow will be enormous. However, contrarily, the spectrum allocated by some countries for wireless communication seems to be insufficient to supply such a rich range of applications. For instance, the FCC only allocated 75 MHz of licensed spectrum for DSRC, which is insufficient for Big Data applications.

- High mobility and dynamic density: mobility and density dynamism are among the core differences between IoV and VANETs with other common networks. A highway can lead to a "smoother" network since cars are moving along the road at an expected maximum speed, and, usually, highways are building to be easy to drive. Nevertheless, in cities, the opposite is expected as traffic jams are widespread. As a global challenge, all applications and services will suffer while this issue is not surpassed.

Other specific problems can arise in the Big Data era in emerging vehicular environments. For example, to mitigate problems related to data and computationally hunger applications and services, computing paradigms could adopt an offloading layer. The offloading idea relies on the transfer of storage or computation to capable network elements, in a particular moment, which can fulfill more efficiently such duty, either because they were previously in the idle state compared to other elements or are merely more powerful to do so [81]. This, however, does not mean that the total mitigation of the problem because there is still a lack of ubiquitous networks and powerful enough nodes. Please note that more information can be found in [82]–[84].

B. Challenges

As previously mentioned, the dynamism of the network topology is the first big challenge. Protocols that provide security while considering the unstable network structure must be specially tailored for vehicular environments [85], [86]. This is valid for both IoV and VANET. The latter networks still lack a set of standards for their various layers.

Nowadays' adoption of 5G and WAVE only solves part of the whole set of features for vehicular environments. The so-called best practices for the development of services and applications also do not exist yet. The primary impulse to solve them will come when these networks start to be widely used in everyday life worldwide, particularly IoV.

Recent works aim to use Big Data, AI, Blockchain, and Software Defined Networks (SDN) to address some challenges of vehicular networks. For instance, Big Data's use can be as valuable as saving more lives by anticipating congestions and accidents, a challenge for ITS and VANET [87]. Z. Zhou et al. [88] address content distribution challenges with a heuristic scheme using Big Data and coalition game behavior for VANETs.

AI can be used for a variety of reasons in vehicular environments ranging from network to driver benefits [89]. For example, if we are using Big Data services, it is necessary to distribute the computing the network can do with data reliably. Z. Ning et al. [90] try to solve the latter using Deep Reinforcement Learning together with 5G to offload Big Data traffic.

On the top layer of IoV, multimedia services and applications usually need QoS, a way to quantify how nearer to an ideal or expected scenario the network delivers these services. A. H. Sodhro et al. [91] use AI to provide optimization in QoS for IoV communications. A. H. Sodhro et al. [92] propose a self-adaptative, reliable, intelligent, and mobility-aware intra-vehicular mobility management algorithm for vehicular fog networks to avoid interference so that the network provides seamless connection. Moreover, F. Tang et al. [93] discuss the possible applications and challenges future vehicular networks will have using 6G and Artificial Intelligence.

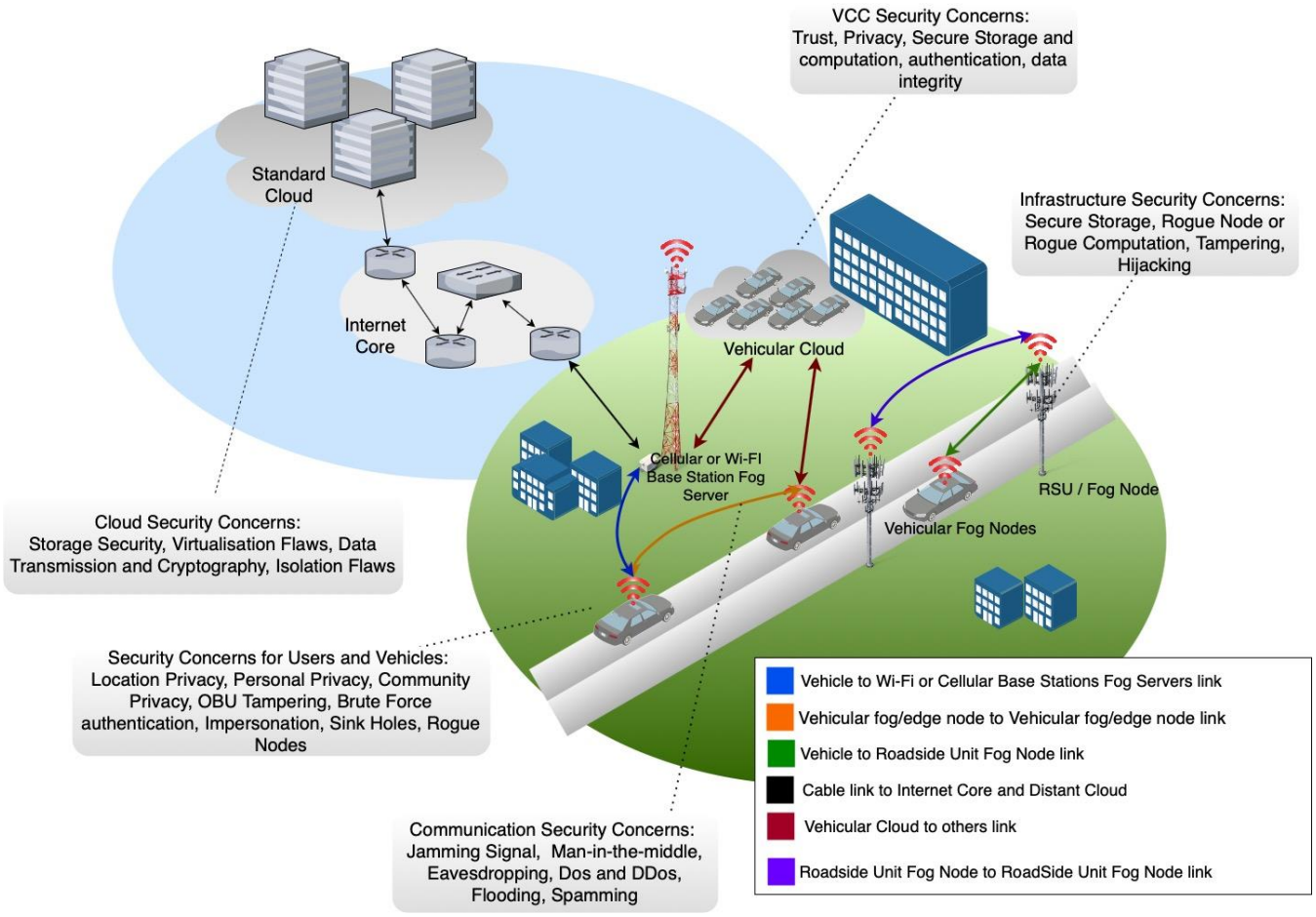


Fig. 4. Security concerns in vehicular environment architectures

Regarding Blockchain, the authors [94] and [95] focus on vehicular environments' challenges related to strong, traceable, and reliable data sharing, and dissemination, and scalable secure protocols. Also, authentication schemes that guarantee network participants' security is a fundamental challenging aspect [96].

W. Zhuang et al. [97] discuss SDN's ability to address the challenges IoV services have, namely offloading tasks, mobility-aware computation, caching deployment and dissemination, and more.

In the next section, we will talk about security issues. They are, to some extent, linked to the limitations and challenges presented here, and hence fundamental to tackle.

VI. Security Issues

With the possibility of using different types of services and the ability to exchange information with different entities that integrate the vehicular networks, the need to improve security solutions is mandatory for the proper functioning of the network. The increase of such services means more data exchange that, ultimately, is correlated to each of the participants, and therefore, considered sensitive.

X. Wang et al. [98] [99] address privacy issues for messages exchanged in the network in a specific case, i.e., vehicular social networks (VSN – a new paradigm centered in the social properties of vehicular networks to improve their performance), and a much broader sense. N. Magaia et al. [100][101] proposed privacy-preserving routing protocols to conceal routing metrics necessary in such networks.

Despite all VSN characteristics, data dissemination, attacks, and the possible mitigations, when talking about privacy, the following issues exist:

- Location and trace privacy: There are roughly two layers of location-based services: the first one is for safety applications, thus thought of as a service provided by the control channel. It will be developed in secure protocols. However, the second one is more general-purpose, as when a driver wants to know where the nearest place with a gas station is. Here, the location providers cannot provide adequate protocols to maintain driver's privacy, besides being an open question if they will share it or not with third parties, similarly to what happens on the Internet.
- Personal and common interest privacy: despite the roads being a common path in which people of different interests go along to reach several different places, and while traveling, they tend to share interests in order to maintain a welfare state. These interests can be categorized in such a way, for a

vehicular network, they can help to shape traffic. However, these groups of interest should not be supposedly leaked. This is the common interest of privacy and can be considered by vehicular network protocols.

- Community privacy: This more general privacy requirement stands for the fact that one malicious user can trace other user's personal information based on what virtual communities they are in. As an example, a wealthy community user can be exposed and targeted if the VSN is not able to keep private the marketplaces that the user goes.

For both VSN, Social IoV, and Big Data content exchange (i.e., a novel concept briefly discussed in the previous section), security issues are still open.

There are general security aspects and the specific ones to a particular technology, application, or service. The three fundamental security requirements are confidentiality, integrity, and availability (CIA) [102][103], besides, there are authentication, non-repudiation, privacy and anonymity, traceability and revocability, data verification, and access control, which are relevant in the context of VANETs [104], for example.

For the specific security issues, we know that security is also something directly related to the design of what is being analyzed; hence it is common to list characteristics and possible associated security problems.

Table 2, Table 3, Table 4, and Table 5 gather characteristics and possible security issues surveyed from the most recent literature of VANETs [104], IoVs [105], cloud [106]–[109], and fog computing [110]–[114].

Please note that instead of listing VCC and VFC issues, we could have mentioned cloud and fog computing ones since we believe, except the environment, they share similar problems, differing only in the cyber-physical elements that compose them.

For example, in a traditional cloud, there is a set of geographically distributed computers offering services, and in the case of the VCC, this set is formed by vehicles.

For both VANET and IoV, plenty of communication attacks can happen not only because these networks are still in exhaustive development but their actual implementation, commercially speaking, are not guaranteed to bring the security countermeasures that are researched/proposed [115]–[117].

Like any network, VANET and IoV could suffer from signal jamming, man-in-the-middle attacks, eavesdropping, spoofing, flooding, spamming, DoS, and DDoS attacks. One can even try to tamper OBUs or access the vehicle internals through the network interface since it can happen to exist a link within the underlying OS running in it [118].

These problems escalate when in an IoV network as vehicle sensors and engines, user peripherals, and devices are supposed to act together to deliver a pleasant and unified experience and servicing to vehicle users or owners. Each of these devices brings their issues, and their expected "organic" communication opens the door to how much an attacker can go hopping from point to point inside the IoV structure.

For VFC and VCC, the same myriad of problems as above happens, but also each vehicle, and each infrastructure element, as a node, can behave in such a way that it is designed rogue node because it either exhaustively uses VFC or VCC computing power to some malicious intent, or stay still tampering and scavenging data passing through. Ultimately, attackers will modify their vehicle to use it as a malicious weapon as much as fake Access Points are a common issue in coffee shops.

Table 6 presents common attacks and possible solutions in vehicular networks.

It is out of this work's scope to present an exhaustive coverage of the security problems and solutions in vehicular environments since they are already available in the literature [119].

It is also vital to highlight tradeoffs as if, on the one hand, using technology or paradigm implies being susceptible to all the risks of its logical and implementation failures. On the other hand, it allows using those very technologies or paradigms to mitigate other problems.

The following examples present the use of VANETs, IoV, VCC, and VFC and their security benefit. M. Bousselham et al. [120] and S. K. Erskine and K. M. Elleithy [121] suggest how to use fog computing to enhance VCC and VANETs security, respectively. In R. Hussain and H. Oh [122], cooperation-as-a-service and VANET Clouds are used for security in the VANETs themselves. Additionally, in R. Hussain et al. [123], 5G is used with VANETS to increase network security following a top-down approach. K. Xue et al. [124] present an architecture incrementing privacy and data-sharing in VCCs using a fog-to-cloud scheme.

Fig. 4 presents security concerns in vehicular environment architectures.

VII. Future Directions

The implementation of computing paradigms in vehicular environments such as VCC and VFC (or VEC) is still in development, conversely to cloud computing, whose concept dates back to the 1960s [125], [126]. In the last ten years, we have seen computers being used as a source of services with the "illusion" of an infinite amount of resources; meanwhile, fog computing is quite a recent concept [62].

Currently, and even though it is a time of transition, vehicular networks, in particular, IoVs, are not popular, nor even the commercialization of 5G networks, which are expected to be implemented in 2020 [4]. Although there are already VANETs, which realize some ITS use cases, they do not exist in the same order of magnitude as IoT or the adoption of smartphones, which already have around 20.8 billion devices [127].

In computing, it is common for there to be a stage of development of the physical layer. The following layers and logical abstractions come to make the infrastructure available in an almost transparent way so that even people who know little or nothing about that infrastructure can create services and applications. This departure from the structural layer to the highest level often allows the construction of what is called the Intelligence of something, which is when "ordinary" people

have the opportunity to develop their services, and innovations happen.

Therefore, we present what we believe will help achieve the "ubiquitous" status desired for vehicular networks and networks in general.

Below, we present the following three required elements:

- Software-Defined Networking (SDN) [128]: SDNs are a way of seeing and, therefore, of structuring the network so that its programmability is enhanced by separating the data and control planes. This flexibility makes, for example, a device with SDN capability capable of functioning as a switch, firewall, or router using, for instance, OpenFlow or P4 [129]. SDNs are used for multiple purposes, such as in data centers. H. Yuan et al. [130] give an example of how data centers and VCC can benefit from SDNs. They considered the inherent latency of virtual machines and formulated the Workload-Aware Multi-Application (WARM) method to optimize the distribution of data and tasks to virtual machines through optimal paths for each. The result of load balancing is effectively better with a decrease of the Round-Trip Time (RTT) compared to other know methods. Vehicles' OBUs will need to have intelligence capabilities, a high transmission rate, and, most probably, SDN functionalities. The latter will enable vehicles, whether participating in the cloud or as fog nodes, to shape the network more flexibly, participating in it more effectively by behaving as components not only of the network edge but also of its core. An architecture can be found in [131].
- 6th generation mobile networks [132], [133]: Each generation of cellular technology has a forecast of application creation between 10 to 20 years. Although 5G networks are already being deployed worldwide, their maturation is expected by 2025/26 and the complete adoption by the year 2030, which will coincide with the beginning of 6G networks [129]. Such networks are promised to have peak data-rates as high a 1 Tbps and enable user-experience data rates as high as 1 to 10 Gbps. Moreover, latency inferior to 1 ms, with expected device positioning precision as low as 10 cm indoors and 1 m outdoors. 6G networks are aimed to be efficient, targeting Green Cities and Computing [132], [134]–[136], with an expected energy efficiency around 100 times higher, spectrum efficiency at least 5 to 10 times higher, and traffic capacity around 1000 times higher than 4G, respectively.
- Serverless computing [137]: In this type of computing, which is directed to the cloud (and possibly fog), there is a drastic change in the way services are performed. In the traditional model, known as serverful, the cloud services are offered in several forms, i.e., IaaS, PaaS, SaaS. However, a user pays for up to a certain amount for resources and cannot surpass it unless he pays more (an upgrade). In the serverless model, functions are executed once at a time from an event-driven perspective. There are three primary characteristics: (i) decoupled computation and storage, and both will possibly be placed in different parts of the cloud or clouds in order to climb in different ways. Therefore, each is charged and priced according to use, and the computing will then be stateless (which will increase virtualization and isolation); (ii) code without resource allocation, not only are computation and storage separated, but the user does not need to define how many resources should be allocated. The cloud will automatically take care of this for each time a function that is triggered; (iii) proportional payment by use, not allocation, the user delivers his code, and the cloud executes it by automatically configuring everything necessary without the user having to specify any information. Then, there is the amount to pay for the time the code needs to run. In short, Serverless computing will enable content, service, or application producers to offer their ideas in such a way to form a new economy around cloud computing, and consequently VCC, and also will give cloud providers much more flexibility to charge for cloud services.

We envisage a future in which billions of devices will form an Internet-of-Everything (IoE) even before 2050. IoE will include vehicles, smartphones, home appliances, smart houses, smart cities, ITS, wearables (internal and external), among others. We also foresee the realization of energy savings through green computing and network processes [132], [134] applied to smart cities [136] and the cloud [138], in order to adapt computing to the immense amount of data that will be on the go continuously feeding real-time systems, and high-quality and faithful video and audio streams.

For the next decade, we realize that in due course, 6G and IoV will possibly have commercial applications. It will also be the time when Serverless Computing will come into operation. It is therefore crucial that researches start uniting VCC, VFC, Serverless Computing, SDNs, and, possibly, 6G as soon as the enabling technologies become commercially viable, thus decreasing latency to the order of pico-seconds meanwhile increasing transmission rates to the order of Terabits per second [133]. It is essential that the Serverless Computing is applied to vehicular networks due to the need for an abstraction between physical elements and their components, which will allow users to create their services. In addition, pricing, whether for users "lending" their vehicles or using others, will be more appropriate, based on time of use and not by the package, something that would be necessarily inappropriate in a dynamic network such as the vehicular one.

The union of these technologies and paradigms seems to us as the natural way to overcome, in the coming years, the difficulties of integrating vehicular networks and making them more user-friendly for programmers who want to develop applications and services. Specifically, it is our conviction that they will mitigate nowadays challenges, i.e., 6G will enable complete ubiquitous network across heterogeneous devices (vehicles, sensors, IoT, Unmannered Aerial Vehicles – UAVs, wearables, among others) at high speeds and very low latency; Serverless Computing will provide sufficient decoupling from the cloud infrastructure so that services can be charged on a

different and easier basis; besides, SDN-enabled network elements will easy to combination and/or complement various computing paradigms in vehicular networks.

VIII. Conclusions

We presented a unifying perspective of technologies, architectures, and nomenclatures concerning computing paradigms in vehicular environments. We believe that the future of vehicular communications will benefit from 5G networks for the next decade, and of 6G after that, besides the Wi-Fi technology. IoVs are considered an evolution of VANET, without disregarding the latter's instrumental role from a safety point of view meanwhile the former's role in providing various services even outside the scope of vehicular environments, in addition to the massive amounts of data analytics in the long run. Even if IoVs are still under research hence not being seen recurrently in cities, their deployment will happen soon. Future safer driving is imperative, and every technological advance is expected to bring more quality of life to people, besides saving lives.

References

[1] R. Sánchez-Corcuera *et al.*, "Smart cities survey: Technologies, application domains and challenges for the cities of the future," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 6, 2019.

[2] L. Zhao *et al.*, "Vehicular Communications: Standardization and Open Issues," *IEEE Commun. Stand. Mag.*, vol. 2, no. 4, pp. 74–80, Dec. 2018.

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

[4] A. N. Barreto *et al.*, "5G – Wireless Communications for 2020," *J. Commun. Inf. Syst.*, vol. 31, no. 1, pp. 146–163, 2016.

[5] M. S. Afaqui, E. Garcia-Villegas, and E. Lopez-Aguilera, "IEEE 802.11ax: Challenges and Requirements for Future High Efficiency WiFi," *IEEE Wirel. Commun.*, vol. 24, no. 3, pp. 130–137, 2016.

[6] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," *IEEE Veh. Technol. Conf.*, no. June 2008, pp. 2036–2040, 2008.

[7] A. Festag, "Standards for vehicular communication—from IEEE 802.11p to 5G," *Elektrotechnik und Informationstechnik*, vol. 132, no. 7, pp. 409–416, 2015.

[8] E. Comission, "COMMISSION DELEGATED REGULATION Directive 2010/40/EU," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.

[9] A. Bazzi, G. Cecchini, M. Menarini, B. M. Masini, and A. Zanella, "Survey and perspectives of vehicular Wi-Fi versus sidelink cellular-V2X in the 5G era," *Futur. Internet*, vol. 11, no. 6, pp. 1–20, 2019.

[10] M. Slovick, "DSRC vs. C-V2X: Looking to Impress the Regulators," *Electron. Des.*, pp. 1–4, 2017.

[11] A. Molinaro and C. Campolo, "5G for V2X Communications," in *The 5G Italy Book 2019: a Multiperspective View of 5G*, M. A. Marsan, N. B. Melazzi, S. Buzzi, and S. Palazzo, Eds. cnit, 2019, pp. 2–6.

[12] C. Voigt, "5G Automotive Association Pioneering the transformation in the automotive industry," 2018.

[13] 5G Automotive Association, "V2X Functional and Performance Test Report ; Test Procedures and Results," no. October, pp. 1–121, 2018.

[14] J. Yoshida, "The DSRC vs 5G Debate Continues," *EET Asia*, 2019. [Online]. Available: https://www.eetasia.com/news/article/The-DSRC-vs-5G-Debate-Continues.

[15] ABI research, "V2X System Cost Analysis: Dsrc+Lte and C-V2X+Lte," p. 9, 2018.

[16] T. Hasegawa, "Chapter 5-Intelligent Transport System," *Traffic Saf. Sci. - Interdiciplinary Wisdom IATSS*, p. 212, 2015.

[17] M. M. Ishaque and R. B. Noland, "Making roads safe for pedestrians or keeping them out of the way? An historical perspective on pedestrian policies in Britain," *J. Transp. Hist.*, vol. 27, no. 1, pp. 115–137, 2006.

[18] L. Figueiredo, I. Jesus, J. A. Tenreiro Machado, J. Rui Ferreira, and J. L. Martins De Carvalho, "Towards the development of intelligent transportation systems," *IEEE Conf. Intell. Transp. Syst. Proceedings, ITSC*, no. 81, pp. 1206–1211, 2001.

[19] S. Makino, Hiroshi; Kamijo, "Intelligent Transport Systems (ITS)," vol. 1, pp. 1–38, 2016.

[20] ETSI, "ETSI TR 102 638 V1.1.1 (2009-06): Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions," *ETSI, Sophia Antip. Cedex, Fr.*, vol. 1, pp. 1–81, 2009.

[21] S. Mandžuka, "Intelligent transport systems," *A Dict. Transp. Anal.*, pp. 210–214, 2010.

[22] M. Moustafa, Hassnaa; Senouci, Sidi Mihammed; Jerbi, "Introduction to Vehicular Networks," *SpringerBriefs Comput. Sci.*, no. 9781461493563, pp. 1–8, 2013.

[23] M. Alsabaan, W. Alasmary, A. Albasir, and K. Naik, "Vehicular networks for a greener environment: A survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 3, pp. 1372–1388, 2013.

[24] V. Jindal and P. Bedi, "Vehicular Ad-Hoc Networks: Introduction, Standards, Routing Protocols and Challenges," *Int. J. Comput. Sci. Issues*, vol. 13, no. 2, pp. 44–55, 2016.

[25] F. Arena and G. Pau, "An overview of vehicular communications," *Futur. Internet*, vol. 11, no. 2, 2019.

[26] M. S. Sheikh, L. Jun, and W. Wang, "A Survey of Security Services , Attacks ," *sensors Rev.*, vol. 19, 2019.

[27] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, 2018.

[28] O. Kaiwartya *et al.*, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[29] N. Magaia and Z. Sheng, "ReFIoV: A novel reputation framework for information-centric vehicular applications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1810–1823, 2019.

[30] K. Golestan, R. Soua, F. Karray, and M. S. Kamel, "Situation Awareness Within the Context of Connected Cars," *Inf. Fusion*, vol. 29, no. C, pp. 68–83, May 2016.

[31] GSMA, "Connected Society The State of Mobile Internet Connectivity 2019," *comScore Mobilens*, pp. 01–56, 2019.

[32] GSMA, "GSMA The Mobile Economy 2019 - The Mobile Economy," *GSMA*, 2019. [Online]. Available: https://www.gsma.com/r/mobileeconomy/%0Ahttps://www.gsma.com/r/mobileeconomy/sub-saharan-africa/%0Ahttps://www.gsma.com/r/mobileeconomy/.

[33] N. Safety Council, "Injury Facts: The Source for Injury Stats," *Injury Facts*, 2020. [Online]. Available: https://www.nsc.org/membership/member-resources/injury-facts.

[34] ERSO, "Annual Accident Report 2018, European Road Safety Observatory," pp. 1–86, 2018.

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

[36] Z. Ning *et al.*, "Deep Learning in Edge of Vehicles: Exploring Trirelationship for Data Transmission," *IEEE Trans. Ind. Informatics*, vol. 15, no. 10, pp. 5737–5746, 2019.

[37] W. J. Chang, L. B. Chen, and K. Y. Su, "DeepCrash: A deep learning-based internet of vehicles system for head-on and single-vehicle accident detection with emergency notification," *IEEE Access*, vol. 7, pp. 148163–148175, 2019.

[38] P. Mell and T. Grance, "The NIST-National Institute of Standars and Technology- Definition of Cloud Computing," *NIST Spec. Publ. 800-145*, p. 7, 2011.

[39] M. Vaquero, Luis M.; Rodero-Merino, Luis; Caceres, Juan; Lindner, "A Break in the Clouds: Towards a Cloud Definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2009.

[40] T. Dillon, C. Wu, and E. Chang, "Cloud computing: Issues and challenges," in *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, 2010, pp. 27–33.

[41] R. Grozev, Nikolay; Buyya, "Inter-Cloud architectures and

application brokering: taxonomy," *Softw. - Pract. Exp.*, vol. 44, pp. 369–390, 2014.

[42] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Futur. Gener. Comput. Syst.*, vol. 79, pp. 849–861, 2018.

[43] J. Wan, C. Zou, K. Zhou, R. Lu, and D. Li, "IoT sensing framework with inter-cloud computing capability in vehicular networking," *Electron. Commer. Res.*, vol. 14, no. 3, pp. 389–416, Dec. 2014.

[44] I. Odun-Ayo, M. Ananya, F. Agono, and R. Goddy-Worlu, "Cloud Computing Architecture: A Critical Analysis," in *Proceedings of the 2018 18th International Conference on Computational Science and Its Applications, ICCSA 2018*, 2018.

[45] R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: Utility-oriented federation of cloud computing environments for scaling of application services," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6081 LNCS, no. PART 1, pp. 13–31.

[46] M. Vukoli, "The byzantine empire in the intercloud," *ACM SIGACT News*, vol. 41, no. 3, p. 105, Sep. 2010.

[47] A. J. Ferrer, "Inter-cloud Research: Vision for 2020," in *Procedia Computer Science*, 2016, vol. 97, pp. 140–143.

[48] M. Liaqat *et al.*, "Federated cloud resource management: Review and discussion," *J. Netw. Comput. Appl.*, vol. 77, no. May 2016, pp. 87–105, 2017.

[49] J. W. Rittinghouse and J. F. Ransome, *Cloud computing : implementation, management, and security*. CRC Press, 2010.

[50] I. Costa, J. Araujo, J. Dantas, E. Campos, F. A. Silva, and P. Maciel, "Availability Evaluation and Sensitivity Analysis of a Mobile Backend-as-a-service Platform," *Qual. Reliab. Eng. Int.*, vol. 32, no. 7, pp. 2191–2205, 2016.

[51] C. Curino *et al.*, "Relational cloud: A database-as-a-service for the cloud," *CIDR 2011 - 5th Bienn. Conf. Innov. Data Syst. Res. Conf. Proc.*, pp. 235–240, 2011.

[52] P. Costa, M. Migliavacca, and A. L. Wolf, "NaaS : Network-as-a-Service in the Cloud," *2nd USENIX Work. Hot Top. Manag. Internet, Cloud, Enterp. Networks Serv.*, pp. 1–6, 2012.

[53] L. Lavazza, R. Oberhauser, R. Koci, C. Republic, and S. Clyde, *Icsea 2017*. 2017.

[54] J. Bi *et al.*, "Application-Aware Dynamic Fine-Grained Resource Provisioning in a Virtualized Cloud Data Center," *IEEE Trans. Autom. Sci. Eng.*, vol. 14, no. 2, pp. 1172–1184, 2017.

[55] H. Yuan, J. Bi, W. Tan, M. C. Zhou, B. H. Li, and J. Li, "TTSA: An Effective Scheduling Approach for Delay Bounded Tasks in Hybrid Clouds," *IEEE Trans. Cybern.*, vol. 47, no. 11, pp. 3658–3668, 2017.

[56] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog Computing: Principles, architectures, and applications," *Internet Things Princ. Paradig.*, pp. 61–75, 2016.

[57] OpenFog Consortium Architecture Working Group, "OpenFog Reference Architecture for Fog Computing," *OpenFog*, no. February, pp. 1–162, 2017.

[58] E. Wikström and U. M. Emilsson, "Autonomy and Control in Everyday Life in Care of Older People in Nursing Homes," *J. Hous. Elderly*, vol. 28, no. 1, pp. 41–62, 2014.

[59] J. Xu, K. Ota, and M. Dong, "A real plug-and-play fog: Implementation of service placement in wireless multimedia networks," *China Commun.*, vol. 16, no. 10, pp. 191–201, 2019.

[60] P. Y. Zhang, M. C. Zhou, and G. Fortino, "Security and trust issues in Fog computing: A survey," *Futur. Gener. Comput. Syst.*, vol. 88, pp. 16–27, 2018.

[61] W. Yu *et al.*, "A Survey on the Edge Computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2017.

[62] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A Taxonomy, Survey and Future Directions," pp. 103–130, 2018.

[63] R. K. Naha *et al.*, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018.

[64] M. Gushev, "Dew Computing Architecture for Cyber-Physical Systems and IoT," *Internet of Things*, vol. 11, p. 100186, 2020.

[65] M. Uehara, "Mist Computing: Linking Cloudlet to Fogs," *Stud. Comput. Intell.*, vol. 726, pp. 201–213, 2018.

[66] W. Shi, "The Emergence of Edge Computing," no. 0018, pp. 17–20, 2016.

[67] U. Shaukat, E. Ahmed, Z. Anwar, and F. Xia, "Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges," *J. Netw. Comput. Appl.*, vol. 62, pp. 18–40, 2016.

[68] 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, 2014.

[69] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking Vehicular Communications: Merging VANET with cloud computing," in *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 2012, pp. 606–609.

[70] M. Sookhak *et al.*, "Fog Vehicular Computing: Augmentation of Fog Computing Using Vehicular Cloud Computing," *IEEE Veh. Technol. Mag.*, vol. 12, no. 3, pp. 55–64, 2017.

[71] H. A. Khattak, S. U. Islam, I. U. Din, and M. Guizani, "Integrating Fog Computing with VANETs: A Consumer Perspective," *IEEE Commun. Stand. Mag.*, vol. 3, no. 1, pp. 19–25, 2019.

[72] M. Satyanarayanan, "The emergence of edge computing," *Computer (Long. Beach. Calif).*, vol. 50, no. 1, pp. 30–39, 2017.

[73] L. Liu, C. Chen, Q. Pei, S. Maharjan, and Y. Zhang, "Vehicular Edge Computing and Networking: A Survey," vol. XX, no. Xx, pp. 1–19, 2019.

[74] L. Tuyisenge, M. Ayaida, S. Tohme, and L. E. Afilal, "Network Architectures in Internet of Vehicles (IoV): Review, Protocols Analysis, Challenges and Issues," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 11253 LNCS, pp. 3–13.

[75] 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, 2019.

[76] V. Fux, P. Maillé, and M. Cesana, "Price competition between road side units operators in vehicular networks," *2014 IFIP Netw. Conf. IFIP Netw. 2014*, 2014.

[77] 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.

[78] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, "Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures," *IEEE Trans. Veh. Technol.*, vol. 65, no. 6, pp. 3860–3873, 2016.

[79] V. G. Menon, "Moving From Vehicular Cloud Computing to Vehicular Fog Computing:Issues and Challenges," *Int. J. Comput. Sci. Eng.*, vol. 2, no. 2, pp. 14–18, 2017.

[80] W. Xu *et al.*, "Internet of vehicles in big data era," *IEEE/CAA J. Autom. Sin.*, vol. 5, no. 1, pp. 19–35, 2018.

[81] D. Xu *et al.*, "A survey of opportunistic offloading," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 3, pp. 2198–2236, 2018.

[82] A. B. De Souza, P. A. Leal Rego, and J. N. De Souza, "Exploring Computation Offloading in Vehicular Clouds," *Proceeding 2019 IEEE 8th Int. Conf. Cloud Networking, CloudNet 2019*, vol. 1, pp. 12–15, 2019.

[83] F. Rebecchi, M. Dias De Amorim, V. Conan, A. Passarella, R. Bruno, and M. Conti, "Data offloading techniques in cellular networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 2, pp. 580–603, 2015.

[84] M. Gong and S. Ahn, "Computation Offloading- Based Task Scheduling in the Vehicular Communication Environment for Computation-Intensive Vehicular Tasks," *2020 Int. Conf. Artif. Intell. Inf. Commun. ICAIIC 2020*, pp. 534–537, 2020.

[85] O. Senouci, Z. Aliouat, and S. Harous, "A review of routing protocols in internet of vehicles and their challenges," *Sens. Rev.*, vol. 39, no. 1, pp. 58–70, 2019.

[86] 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.

[87] H. Al Najada and I. Mahgoub, "Anticipation and alert system of congestion and accidents in VANET using Big Data analysis for Intelligent Transportation Systems," *2016 IEEE Symp. Ser. Comput. Intell. SSCI 2016*, 2017.

[88] Z. Zhou *et al.*, "Trajectory-Based Reliable Content Distribution in D2D-Based Cooperative Vehicular Networks: A Coalition Formation Approach," *IEEE Int. Conf. Commun.*, vol. 2018-May, no. 3, pp. 953–964, 2018.

[89] P. Gomes, N. Magaia, and N. Neves, “Industrial and artificial internet of things with augmented reality,” in *Internet of Things*, Springer, 2020, pp. 323–346.

[90] Z. Ning *et al.*, “When Deep Reinforcement Learning Meets 5G-Enabled Vehicular Networks: A Distributed Offloading Framework for Traffic Big Data,” *IEEE Trans. Ind. Informatics*, vol. 16, no. 2, pp. 1352–1361, 2020.

[91] A. H. Sodhro, Z. Luo, G. H. Sodhro, M. Muzamal, J. J. P. C. Rodrigues, and V. H. C. de Albuquerque, “Artificial Intelligence based QoS optimization for multimedia communication in IoV systems,” *Futur. Gener. Comput. Syst.*, vol. 95, pp. 667–680, 2019.

[92] A. H. Sodhro, G. H. Sodhro, M. Guizani, S. Pirbhulal, and A. Boukerche, “AI-Enabled Reliable Channel Modeling Architecture for Fog Computing Vehicular Networks,” *IEEE Wirel. Commun.*, vol. 27, no. 2, pp. 14–21, 2020.

[93] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, “Future Intelligent and Secure Vehicular Network Toward 6G: Machine-Learning Approaches,” *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, Feb. 2020.

[94] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, “Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory,” *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, 2019.

[95] U. Javaid, M. N. Aman, and B. Sikdar, “A Scalable Protocol for Driving Trust Management in Internet of Vehicles with Blockchain,” *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2020.

[96] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, “An improved authentication scheme for internet of vehicles based on blockchain technology,” *IEEE Access*, vol. 7, pp. 45061–45072, 2019.

[97] W. Zhuang, Q. Ye, F. Lyu, N. Cheng, and J. Ren, “SDN/NFV-Empowered Future IoV with Enhanced Communication, Computing, and Caching,” *Proc. IEEE*, vol. 108, no. 2, pp. 274–291, 2020.

[98] X. Wang *et al.*, *Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions*, vol. 21, no. 2. IEEE, 2019.

[99] X. Wang *et al.*, “A Privacy-Preserving Message Forwarding Framework for Opportunistic Cloud of Things,” *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5281–5295, 2018.

[100] N. Magaia, C. Borrego, P. Pereira, and M. Correia, “PRIVO: A privacy-preserving opportunistic routing protocol for delay tolerant networks,” in *2017 IFIP Networking Conference (IFIP Networking) and Workshops*, 2017, pp. 1–9.

[101] N. Magaia, C. Borrego, P. R. Pereira, and M. Correia, “EPRIVO: An enhanced PRIvacy-preserving opportunistic routing protocol for vehicular delay-tolerant networks,” *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11154–11168, 2018.

[102] J. Blackley, J. Peltier, and T. Peltier, “Information Security Fundamentals,” *Inf. Secur. Fundam.*, 2004.

[103] N. Magaia, P. Rogerio Pereira, and M. P. Correia, “Security in Delay-Tolerant Mobile Cyber Physical Applications,” in *Cyber-Physical Systems: From Theory to Practice*, D. B. Rawat, J. J. P. C. Rodrigues, and I. Stojmenovic, Eds. CRC Press, 2015, pp. 373–394.

[104] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, “VANet security challenges and solutions: A survey,” *Veh. Commun.*, vol. 7, pp. 7–20, 2017.

[105] N. Sharma, N. Chauhan, and N. Chand, “Security challenges in Internet of Vehicles (IoV) environment,” *ICSCCC 2018 - 1st Int. Conf. Secur. Cyber Comput. Commun.*, pp. 203–207, 2018.

[106] S. Singh, Y. S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” *J. Netw. Comput. Appl.*, vol. 75, pp. 200–222, 2016.

[107] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[108] M. A. Muller, I; Grundy, J; Morsy, “An Analysis of the Cloud Computing Security Problem,” *Int. Surg.*, vol. 47, no. 3, pp. 288–290, 2014.

[109] V. Chang and M. Ramachandran, “Towards Achieving Data Security with the Cloud Computing Adoption Framework,” *IEEE Trans. Serv. Comput.*, vol. 9, no. 1, pp. 138–151, 2016.

[110] M. Farhadi *et al.*, “A systematic approach towards security in Fog computing : assets , vulnerabilities , possible countermeasures To cite this version : HAL Id : hal-02441639 A systematic approach towards security in Fog computing : assets , vulnerabilities , possible counte,” 2020.

[111] S. Parikh *et al.*, “Security and Privacy Issues in Cloud , Fog and Edge Computing,” *Procedia Comput. Sci.*, vol. 160, pp. 734–739, 2019.

[112] H. Noura, O. Salman, A. Chehab, and R. Couturier, “Preserving data security in distributed fog computing,” *Ad Hoc Networks*, vol. 94, 2019.

[113] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, “Fog Computing Security Challenges and Future Directions [Energy and Security],” *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 92–96, 2019.

[114] P. Y. Zhang, M. C. Zhou, and G. Fortino, “Security and trust issues in Fog computing: A survey,” *Futur. Gener. Comput. Syst.*, vol. 88, pp. 16–27, 2018.

[115] R. Crook, D. Ince, L. Lin, and B. Nuseibeh, “Security requirements engineering: When anti-requirements hit the fan,” *Proc. IEEE Int. Conf. Requir. Eng.*, vol. 2002-Janua, pp. 203–205, 2002.

[116] B. Duncan, M. Whittington, and V. Chang, “Enterprise security and privacy: Why adding IoT and big data makes it so much more difficult,” *Proc. 2017 Int. Conf. Eng. Technol. ICET 2017*, vol. 2018-Janua, pp. 1–7, 2017.

[117] M. Hossain, R. Hasan, and S. Zawoad, “Trust-IoV: A trustworthy forensic investigation framework for the internet of vehicles (IoV),” *Proc. - 2017 IEEE 2nd Int. Congr. Internet Things, ICIOT 2017*, no. October, pp. 25–32, 2017.

[118] S. Sharma and A. Kaul, “A survey on Intrusion Detection Systems and Honeypot based proactive security mechanisms in VANETs and VANET Cloud,” *Veh. Commun.*, vol. 12, pp. 138–164, 2018.

[119] S. Sharma and B. Kaushik, “A survey on internet of vehicles: Applications, security issues & solutions,” *Veh. Commun.*, vol. 20, p. 100182, 2019.

[120] M. Bousselham, N. Benamar, and A. Addaim, “A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System,” *2019 Int. Conf. Wirel. Technol. Embed. Intell. Syst. WITS 2019*, pp. 1–4, 2019.

[121] S. K. Erskine and K. M. Elleithy, “Secure intelligent vehicular network using fog computing,” *Electron.*, vol. 8, no. 4, 2019.

[122] R. Hussain and H. Oh, “Cooperation-aware VANET clouds: Providing secure cloud services to vehicular Ad Hoc networks,” *J. Inf. Process. Syst.*, vol. 10, no. 1, pp. 103–118, 2014.

[123] R. Hussain, F. Hussain, and S. Zeadally, “Integration of VANET and 5G Security: A review of design and implementation issues,” *Futur. Gener. Comput. Syst.*, vol. 101, pp. 843–864, 2019.

[124] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong, and N. Yu, “Fog-Aided Verifiable Privacy Preserving Access Control for Latency-Sensitive Data Sharing in Vehicular Cloud Computing,” *IEEE Netw.*, vol. 32, no. 3, pp. 7–13, 2018.

[125] D. PARKHILL, “The challenge of the computer,” *JAMA J. Am. Med. Assoc.*, vol. 188, no. 10, pp. 928–929, 1964.

[126] A. Armbrust, “Above the clouds: A Berkeley view of cloud computing,” *University of California, Berkeley, Tech. Rep. UCB*, 2009. [Online]. Available: http://www-inst.cs.berkeley.edu/~cs10/sp11/lec/20/2010Fa/2010-11-10-CS10-L20-AF-Cloud-Computing.pdf%5Cnhttp://scholar.google.com/scholar?q=intitle:Above+the+clouds:+A+Berkeley+view+of+cloud+computing#0.

[127] Y. Xiao and C. Zhu, “Vehicular fog computing: Vision and challenges,” *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 6–9, 2017.

[128] R. Masoudi and A. Ghaffari, “Software defined networks: A survey,” *Journal of Network and Computer Applications*, vol. 67. pp. 1–25, 2016.

[129] S. K. Routray and A. A. Science, “Why 6G ?: Motivation and Expectations of Next- Generation Cellular Networks,” no. March, 2019.

[130] H. Yuan, J. Bi, M. Zhou, and K. Sedraoui, “WARM: Workload-Aware Multi-Application Task Scheduling for Revenue Maximization in SDN-Based Cloud Data Center,” *IEEE Access*, vol. 6, pp. 645–657, 2018.

[131] J. Gao *et al.*, “A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks,” *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4278–4291, 2020.

[132] T. Huang, W. Yang, J. Wu, J. Ma, X. Zhang, and D. Zhang, “A

Survey on Green 6G Network: Architecture and Technologies," *IEEE Access*, vol. 7, pp. 175758–175768, 2019.
[133] 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, 2019.
[134] B. G. Prasuna, M. Sowmya, and P. Prashanti, "Study on G-IoT for Sustainable World," vol. 06, no. 03, pp. 596–600, 2019.
[135] F. Al-Turjman, A. Kamal, M. Husain Rehmani, A. Radwan, and A. S. Khan Pathan, "The Green Internet of Things (G-IoT)," *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019.
[136] K. Muhammad, J. Lloret, and S. W. Baik, "Intelligent and energy-efficient data prioritization in green smart cities: Current challenges and future directions," *IEEE Commun. Mag.*, vol. 57, no. 2, pp. 60–65, 2019.
[137] E. Jonas *et al.*, "Cloud Programming Simplified: A Berkeley View on Serverless Computing," pp. 1–33, 2019.
[138] M. Masdari and M. Zangakani, "Green Cloud Computing Using Proactive Virtual Machine Placement: Challenges and Issues," *J. Grid Comput.*, 2019.
[139] S. Iqbal, A. Haque, and M. Zulkernine, "Towards a security architecture for protecting connected vehicles from malware," *IEEE Veh. Technol. Conf.*, vol. 2019-April, 2019.
[140] L. Nie, Z. Ning, X. Wang, X. Hu, Y. Li, and J. Cheng, "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-based Method," *IEEE Trans. Netw. Sci. Eng.*, vol. 4697, no. c, pp. 1–1, 2020.
[141] Y. Zeng, M. Qiu, D. Zhu, Z. Xue, J. Xiong, and M. Liu, "DeepVCM: a Deep Learning Based Intrusion Detection Method in VANET," in *Proceedings - 5th IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2019, 5th IEEE International Conference on High Performance and Smart Computing, HPSC 2019 and 4th IEEE International Conference on Intelligent Data and Securit*, 2019, pp. 288–293.
[142] H. Liang, J. Wu, S. Mumtaz, J. Li, X. Lin, and M. Wen, "MBID: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection for V2X," *IEEE Commun. Mag.*, vol. 57, no. 10, pp. 77–83, 2019.
[143] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, p. 101842, 2019.
[144] L. Wang and X. Liu, "NOTSA: Novel OBU with Three-Level Security Architecture for Internet of Vehicles," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3548–3558, 2018.
[145] A. Yadav, G. Bose, R. Bhange, K. Kapoor, N. C. S. N. Iyengar, and R. D. Caytiles, "Security, vulnerability and protection of vehicular on-board diagnostics," *Int. J. Secur. its Appl.*, vol. 10, no. 4, pp. 405–422, 2016.
[146] Z. Guo *et al.*, "Robust Spammer Detection Using Collaborative Neural Network in Internet of Thing Applications," *IEEE Internet Things J.*, vol. xx, no. xx, pp. 1–1, 2020.
[147] L. Zhang, X. Meng, K. K. R. Choo, Y. Zhang, and F. Dai, "Privacy-Preserving Cloud Establishment and Data Dissemination Scheme for Vehicular Cloud," *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 3, pp. 634–647, 2020.
[148] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, and M. Guizani, "Evaluating Reputation Management Schemes of Internet of Vehicles Based on Evolutionary Game Theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 6, pp. 5971–5980, 2019.
[149] K. Gu, X. Dong, and W. Jia, "Malicious Node Detection Scheme Based on Correlation of Data and Network Topology in Fog Computing-based VANETs," *IEEE Trans. Cloud Comput.*, vol. 7161, no. c, pp. 1–1, 2020.
[150] K. Zaidi, M. B. Milojevic, V. Rakocevic, A. Nallanathan, and M. Rajarajan, "Host-Based Intrusion Detection for VANETs: A Statistical Approach to Rogue Node Detection," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6703–6714, Aug. 2016.
[151] B. Al-Otaibi, N. Al-Nabhan, and Y. Tian, "Privacy-preserving vehicular rogue node detection scheme for fog computing," *Sensors (Switzerland)*, vol. 19, no. 4, pp. 1–18, 2019.
[152] K. N. Tripathi and S. C. Sharma, "A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS)," *Int. J. Syst. Assur. Eng. Manag.*, vol. 11, no. 2, pp. 426–440, 2020.
[153] M. Alshehri and B. Panda, "Minimizing Data Breach by a Malicious Fog Node within a Fog Federation," pp. 36–43, 2020.
[154] R. Kolandaisamy *et al.*, "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks," *Wirel. Commun. Mob. Comput.*, vol. 2018, 2018.
[155] A. Haydari and Y. Yilmaz, "Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems," *IEEE Conf. Intell. Transp. Syst. Proceedings, ITSC*, vol. 2018-Novem, pp. 157–163, 2018.
[156] Q. Shafi and A. Basit, "DDoS Botnet Prevention using Blockchain in Software Defined Internet of Things," *Proc. 2019 16th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2019*, pp. 624–628, 2019.
[157] K. Adhikary, S. Bhushan, S. Kumar, and K. Dutta, "Hybrid Algorithm to Detect DDoS Attacks in VANETs," *Wirel. Pers. Commun.*, no. 0123456789, 2020.
[158] H. H. R. Sherazi, R. Iqbal, F. Ahmad, Z. A. Khan, and M. H. Chaudary, "DDoS attack detection: A key enabler for sustainable communication in internet of vehicles," *Sustain. Comput. Informatics Syst.*, vol. 23, pp. 13–20, 2019.
[159] Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, "An efficient SDN-Based DDoS attack detection and rapid response platform in vehicular networks," *IEEE Access*, vol. 6, pp. 44570–44579, 2018.
[160] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, 2019.
[161] R. Hussain, H. Oh, and S. Kim, "Antisybil: Standing against sybil attacks in privacy-preserved VANET," *Proc. - 2012 Int. Conf. Connect. Veh. Expo, ICCVE 2012*, pp. 108–113, 2012.
[162] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, "An efficient anonymous authentication scheme for internet of vehicles," *IEEE Int. Conf. Commun.*, vol. 2018-May, pp. 1–6, 2018.
[163] J. Wei, X. Wang, N. Li, G. Yang, and Y. Mu, "A privacy-preserving fog computing framework for vehicular crowdsensing networks," *IEEE Access*, vol. 6, pp. 43776–43784, 2018.
[164] M. A. Saleem, K. Mahmood, and S. Kumari, "Comments on 'AKM-IoV: Authenticated Key Management Protocol in Fog Computing-Based Internet of Vehicles Deployment,'" *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4671–4675, 2020.
[165] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and A. K. Barkaoui, "Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum," *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–27, 2020.

Lion Silva is an MSc student of Computer Science at the Faculty of Sciences of the University of Lisbon. His current research interests cover Internet of Vehicles, Fog/Edge Computing and Network Security.

Naercio Magaia received his Ph.D. in Electrical and Computer Engineering from Instituto Superior Técnico (IST), University of Lisbon (ULisboa). He holds a degree in Electrical Engineering from Eduardo Mondlane University, and an M.Sc. in Communication Networks Engineering from IST, ULisboa. He is currently an Invited Assistant Professor at the Faculty of Sciences of ULisboa and an integrated researcher at the LASIGE research unit. His current research interests cover Computer Networks, Network Security, and Artificial Intelligence.

Breno Sousa received his MSc. in Computer Science with emphasis on Electrical Engineering at Federal University of Maranhão - Brazil. He is currently a researcher fellow at Instituto Dom Luiz of University of Lisbon (ULisboa). His current research interests cover network security, vehicular networks and artificial intelligence.

Anna Kobusinska received her M.Sc., PhD and DSc degrees in computer science from Poznań University of Technology, in 1999, 2006 and 2019, respectively. She currently works as Associate Professor at the Laboratory of Computing Systems, Faculty of Computing and Telecommunications, Poznań University of Technology, Poland. Her research interests include large-scale distributed systems, service-oriented and cloud computing as well as edge computing. In her work, she focuses on distributed algorithms, Big Data analysis, reliability of distributed processing, specifically consistency models and replication techniques, challenges associated with the use of blockchain technology, and the edge intelligence. She has served and is currently serving as a GC, PC and TPC member of several international conferences and workshops. She is also author and co-author of many publications in high quality peer reviewed international conferences and journals. She participated to various research projects supported by national organizations and by EC in collaboration with academic institutions and industrial partners.

António Casimiro is Associate Professor at the Department of Informatics of FCUL, where he joined in 1996.He is a member of the LASIGE research laboratory, where he leads the research line on Cyber-Physical Systems. He has been involved in several international projects, coordinating the KARYON (FP7) and the TRONE (CMU|Portugal) projects. Currently he is involved in the ADMORPH and VEDLIoT H2020 projects, and coordinates the AQUAMON project (FCT). His research has been focusing on architectures, fault tolerance and adaptation in distributed and real-time embedded systems, with applications on cyber-physical systems like autonomous and cooperative vehicles or monitoring and control systems in critical infrastructures. He has more than 80 publications in international refereed journals and conferences and was the program chair of SRDS'14, Ada-Europe'18 and SAFECOMP'20. He coordinates the FCUL's Master in Information Security. He is a member of the IFIP WG10.4 on Dependable Computing and Fault Tolerance, of the Ada-Europe Board, of EWICS TC7, IEEE, ACM, and Ordem dos Engenheiros.

Constandinos Mavromoustakis Mavromoustakis (S'01– M'06–SM'13) is currently a Professor at the Department of Computer Science at the University of Nicosia, Cyprus. He received a five-year dipl.Eng (BSc, BEng, Meng) in Electronic and Computer Engineering from Technical University of Crete, Greece, MSc in Telecommunications from University College of London, UK, and his PhD from the department of Informatics at Aristotle University of Thessaloniki, Greece. Professor Mavromoustakis is leading the Mobile Systems Lab. (MOSys Lab., http://www.mosys.unic.ac.cy/) at the Department of Computer Science at the University of Nicosia and he is the Chair of the IEEE/ R8 regional Cyprus section since Nov. 2019, and since May 2009 he serves as the Chair of C16 Computer Society Chapter of the Cyprus IEEE section. Prof. Mavromoustakis has a dense research work outcome in Mobile and Wearable computing systems and the Internet-of-Things (IoT), consisting of numerous refereed publications including several Books (IDEA/IGI, Springer and Elsevier). He has served as a consultant to many industrial bodies (including Intel Corporation LLC (www.intel.com)), and he is a management member of IEEE Communications Society (ComSoc) Radio Communications Committee (RCC) and a board member the IEEE-SA Standards IEEE SCC42 WG2040.

George Mastorakis received his Ph.D. in Telecommunications from the University of the Aegean, Greece in 2008. He serves as Director of e-Business Intelligence Laboratory and as Associate Professor in the Department of Management Science and Technology at Hellenic Mediterranean University in Greece. His research interests include cognitive radio networks, IoT applications, IoE architectures, radio resource management, Artificial Intelligence applications, networking traffic analysis, 5G mobile networks, dynamic bandwidth management and energy-efficiency networks. He has actively participated in many EU funded research projects (FP6, FP7 and Horizon2020) and national research ones. He has also acted as a technical manager in several research projects funded by GSRT (General Secretariat for Research & Technology, Ministry of Development, Greece). He is editor of nine edited books and author of more than 300 research articles.

Victor Hugo C. de Albuquerque (M'17, SM'19) is a professor and senior researcher at the LAPISCO/IFCE, and ARMTEC Tecnologia em Robótica, Brazil. He has a Ph.D in Mechanical Engineering from the Federal University of Paraíba (UFPB, 2010), an MSc in Teleinformatics Engineering from the Federal University of Ceará (UFC, 2007), and he graduated in Mechatronics Engineering at the Federal Center of Technological Education of Ceará (CEFETCE, 2006). He is a specialist, mainly, in IoT, Machine/Deep Learning, Pattern Recognition, Robotic.