Design Automation for Embedded Systems (2021) 25:237–263
https://doi.org/10.1007/s10617-021-09249-7

Candidate architectures for emerging IoV: a survey and comparative study

Yamina Hichri[1] · **Soumaya Dahi**[2] · **Habib Fathallah**[3]

Received: 13 May 2020 / Accepted: 20 April 2021 / Published online: 12 August 2021

Abstract
Intelligent Transportation System (ITS) is observing significant evolution in terms of technology and investment worldwide. This has given birth to the new concept of Internet of vehicles (IoV) as one of the leading applications of the Internet of Things. IoV aims to offer a better sharing of information and communication between vehicles, enabling higher cooperation for common interests. IoV is increasingly attracting the interest of a significant body of research. The e ort was mostly focused on solving various problems encountered in traditional VANETs, such as lack of coordination between vehicles, insufficient information, scalability, etc. Rapidly, IoV observed, particularly interesting advances taking advantage of exponential growth in communication and data analysis technologies. This includes cloud and/or fog computing, large data analytics, machine learning, and artificial intelligence. In this paper, we make a survey of the existing and recently proposed architecture solutions for IoV systems. Moreover, we define a list of criteria, features, and properties associated to the various architectures in order of making critical and insightful comparisons and assessments. Finally, we outline the key future research perspectives on the topic and define the key technical aspects that will help drive the future of IoV architectures.

Keywords Internet of vehicles · Layered architecture · Software defined networking · Cloud computing · Fog computing · Security

✉ Yamina Hichri
hichriyamina@gmail.com

Soumaya Dahi
soumaya.dahi@supcom.tn

Habib Fathallah
habib.fathallah@gmail.com

[1] Physical and Natural Sciences of Tunis, Faculty of Mathematical, University of Tunis El Manar, 2092 Tunis, Tunisia

[2] Communication Engineering School (Sup'Com), LR11TIC05 MEDIATRON Lab, Faculty of Sciences of Bizerte, University of Carthage, 1083 Tunis, Tunisia

[3] Faculty of Sciences of Bizerte, University of Carthage, Tunis, Tunisia

1 Introduction

1.1 Context and motivations

The Internet of Things (IoT) is used to be defined as connected smart objects that can interact and communicate with each other and with other devices [1, 2]. This concept is stimulating the evolution of vehicular ad hoc networks (VANET) towards the Internet of Vehicles (IoV) paradigm [3]. The basic idea of VANETs considers vehicles as mobile nodes that can communicate to create a network [4]. It is a typical mobile ad hoc network (MANET) in which vehicles are considered as wireless/mobile hotspots, dispersing messages and providing wireless connectivity to other vehicles and humans nearby.

No one can deny VANET's role in traffic management, congestion monitoring/avoidance, and control, through communication between vehicles and road units. However, the vehicle and ITS industry, in addition to the research community, push to extend towards new possibilities, including new services and applications, hence increasing the market potential and footprint. The latter requires establishing communication channels between vehicles, vehicles and people, vehicles and infrastructure, or simply a vehicle and everything. IoV is conceptualized to address some of the weaknesses of the VANETs through providing Internet connectivity. Such connectivity offers the system better information exchange capabilities to facilitate driving, address warnings, share awareness and information about parking, etc. It also offers the socialization of system objects, such as vehicles, infrastructure, passengers, etc. In IoV systems, four types (or models) of communications links are encountered, see Fig. 1. Each of these communication links may have its own characteristics/challenges, whether this involves only vehicles at its ends, or pedestrians, infrastructure, or network nodes/terminals.

A vehicle is regarded the most significant node in an IoV system on which all services are based. It serves simultaneously as a transmitter, receiver, and relay of information. Nevertheless, the dynamicity and the mobility of a vehicle may frequently disrupt its communication channels, preventing it to share/receive information to/from pedestrians, vehicles, and/or infrastructure. Therefore, providing continuous access and exchanging reliable data in real-time are challenging issues when designing an IoV architecture. Moreover, IoV system architectures need to consider several aspects, in order to provide drivers, the information and services they need for safe and comfortable driving.

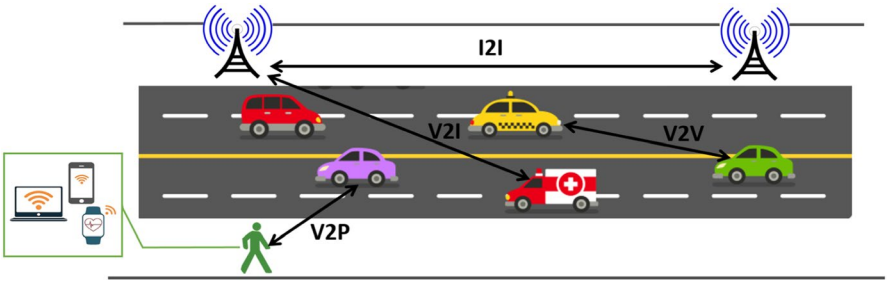

Fig. 1 Inter-networking in IoV: V2V is the wireless transmission of data between vehicles, V2I is the wireless exchange of data between vehicles and road infrastructure, V2P allows direct and exible communication among vehicles and roadside passengers and I2I is the exchange of data between infrastructures

In this work, we surveyed and analyzed most proposed IoV architectures in order to develop an insightful understanding of the core functionalities and the main trends in this specific research topic. We establish a comparative analysis of the various recently proposed architectures and highlight the open challenges. A list of advantages and limitations of the different IoV architectures has also been provided. Multiple criteria of comparison are taken into consideration such as the enabling technologies (Cloud Computing, Fog Computing, SDN, and Context Awareness), security, the number of layers in addition to their key functions and subfunctions. Because of the fast-growing field, this survey work could be extremely beneficial for IoV system designers, standard bodies, and researchers associated with the field. This comparative simulated study might lead to formulate robust and comprehensive judgements about the performance of IoV systems.

1.2 Related work

Despite the importance of the architecture in IoV, a quite limited number of works have been published considering the analysis of the features, the functionalities, and the capabilities with a comparative perspective. In fact, each of the existing works has defined and/or adopted specific architectures by hypothesis and focused on developing other aspects of features in IoV systems. In [5], the authors introduced few-layered IoV architectures and particularly focused on SDN and Fog computing capabilities. In [6], the authors propose an architecture for real-time ITS in IoV system. They particularly focused on real-time Big Data processing requirements. The authors in [4], discussed some proposed architectures for IoV, by evaluating them from a functional point of view, thus showing the efficiency of their proposed architecture. A number of weaknesses in various architectures have been identified. These weaknesses include security issue (authentication, authorization, accounting, and trust relations), integration of the communication intelligence (selection of best network for data transmission/dissemination or service access). The authors have all criticized the interaction with drivers and passengers, which is restricted to, providing notifications through the different car devices.

A Survey taking into consideration a comparative study of VANETs and IoV based on numerous parameters has been investigated in [7]. The study explored the potential applications of IoV in different areas and studied the research challenges as well as security aspects including security attacks and the existing security solutions. IoV Security issues have been also surveyed by Shen et al. [8]. The survey provides an overview of IoV-related technologies and solutions, which address the current challenges, and reveals the potential Advanced IoV Applications. The work of Ji et al. [9] explores a literature review of the basic information and technical background of IoV, including fundamental VANET technology, several network architectures, concepts, models, and typical application of IoV. The development status of network architectures in IoV has been summarized and followed by suggesting a new car-road-cloud collaborative network architecture.

In [10], Kaiwartya et al. discuss the design of the layered architecture of a universal network, including heterogeneous networks. The authors assume that the optimization of the number of layers, the improvement of differentiability among layers, and various network characteristics of the heterogeneous architecture (i.e. interoperability, scalability, reliability, modularity) are the main priorities of the layered architecture design. They admit as well that an open and flexible layered architecture in terms of technology adaptation is more suitable.

The studies mentioned above did not perform a comparative analysis based on a number of key criteria. The authors limited their comparison to only a few aspects that are directly associated with their respective proposals. Various important issues related to security, context awareness, and others, have not been examined. Therefore, in this paper, we provide a comprehensive survey on different technologies utilized for the conception of IoV architectures, along with a list of advantages and limitations of several recently proposed architectures. The study was conducted on the basis of various key aspects and enabling technologies for IoV systems conception such as security, context awareness, real-time processing, Cloud/fog Computing, Content-Centric Networking, etc. Then, the studied literature architectures were analyzed by classifying them according to their number of layers, and evaluated considering the mentioned performance metrics. Moreover, as it is of critical importance in modelling effective IoV systems, we highlight the benefits and identify the pitfalls of numerous IoV architectures. One of the benefits of this survey is to develop a common ground for the various architectures, based on which, the candidate approaches could be evaluated and compared to each other.

1.3 Organization of the paper

The remainder of this paper is organized as follows. Section II illustrates a short overview of Internet of Vehicles (IoV). Section III presents several enabling technologies that will be part of the comparison criteria between candidate architectures. Section IV is dedicated to identifying and detailing a set of key features in existing and recently proposed IoV architectures. In Section V, we illustrate our comparative study between the candidates, identify the critical issues that continue to be open topics for research. The work is concluded in Section VI.

2 Internet of vehicles

2.1 Intelligent transportation system (ITS)

The recent evolutionary trend in both, technology and market, show that Internet of vehicles (IoV) [11] is one of the leading applications of the Internet of Things (IoT) technology. Worldwide, the number of vehicles is expected to be 2 billion by 2030 [12]. Researchers predict that IoV components will produce big data in high speeds. For instance, video data are considered as the biggest big data, which can easily make the IoV data grow to a TB/PB level in seconds [13]. In contrast to VANET, IoV is based on a large scale network that supports services for big cities and a whole country [14]. An IoV is defined as a platform that realizes, in depth, the integration and the data exchange between humans, vehicles, things, and the environment [15]. In fact, IoV is quickly becoming one of the key enabling technology for future intelligent transportation system (ITS) [16]. Industry experts predict that the number of connected cars will increase by 35% by 2021 to reach nearly 280 million vehicles connected on the road [17]. Vehicles are able to intercommunicate independently thanks to a set of external sensors such as the Global Positioning System (GPS), cameras, sensors, and internal automotive actuators (brakes, accelerator, etc.) which collect a wide range of information and transform vehicles into data sources [18]. IoV not only provides wireless communication between a vehicle and other vehicles, roads, pedestrians, and the Internet, but also delivers intelligent traffic management, traffic congestion

detection, infotainment, collision warning, etc. Besides, the US Department of Transportation estimates that connected vehicles can improve safety and eliminate or at least reduce the severity of nearly 80% of road accidents [19].

2.2 Vehicle-to-vehicle (V2V) communication

The main goal of V2V communication is to allow vehicles to communicate and coordinate with each other. Over an ad-hoc mesh network, V2V prevents accidents, makes driving safer and more comfortable, and enables real-time warnings. The shared data include information about vehicle mobility (direction of travel, location, speed, acceleration, etc.), vehicle status (break, CO2 emission, engine, etc.) information about the road (historical accident information, road indication) information about the road weather (ice, fog, snow, rain-slicked road patches, etc.).

2.2.1 Vehicle-to-infrastructure (V2I) communication

It is based on the connection between onboard services and the roadside infrastructure (traffic lights, cameras, streetlights, antennas, sensors, etc.). This is intended to allow drivers to be aware of traffic difficulties, avoid accidents, indicate prone routes and improve safety. A vehicle should be able to exchange the same type of information as in the case of V2V communication, but through fixed communication infrastructure [20].

2.2.2 Vehicle-to-network (V2N) communication

Facilitated by LTE Broadcast, V2N provides over-the-top cloud services, traffic updates, routing, and media streaming. Recently, a widely deployed LTE network has been envisioned to support V2X communication in 3GPP release 14 [21]. V2N applications are supported by a UE and a serving entity, communicating with each other via an LTE network [22].

2.2.3 Vehicle-to-roadside pedestrian (V2P) communication

Despite the fact that the number of road deaths in recent years has been steadily declining, the number of pedestrian and bicycle fatalities has remained relatively constant and represents a significant proportion of the total number of road deaths and injuries [23].

The protection of pedestrians, cyclists, people using wheelchairs and other mobility devices is part of the ongoing e orts of many governments worldwide [24].

IoV was intended primarily to enhance ITS by absorbing environmental information using sensors, to process them using computing units, to store and share them through multiple communication technologies. New technologies such as Vehicular Cloud Computing (VCC), Software defined Networking (SDN), Fog computing, Mobile Edge Computing, Big Data, etc., are seen as mean to provide new, innovative and improved services. In fact, this contributes to the development of more reliable system that meet the needs of drivers to properly manage traffic, provide secure and comfortable driving, avoid congestion, in addition to reduce fuel consumption, carbon emission, and accident frequency. In Table 1, we summarize and compare the characteristics of VANET and IoV.

Table 1 Characteristics of VANET and IoV

Networks	Communications type	Connectivity	Scalability	Cloud compatibility	Environment awareness	Compatibility with personal devices	Processing power and decision capabilities
VANET	V2V, V2R/V2I	Limited (risk of disconnection)	Non-scalable	Limited	Limited	Limited	Limited
IoV	V2X	Always connected	Scalable	Based on CC services	Possible	Any PD	High capabilities

2.3 Future 5G for IoV

The significant increase in the number of connected vehicles requires a high-speed network and minimal latency. The need to deal with large volumes of high-speed and real-time continuous streams of data has been raised by the dynamic nature of IoV [25]. The next generation of mobile broadband, the Fifth Generation (5G) is expected to provide a significant improvement over current 4G LTE standards. This enhancement includes speeds ranging from 300 MB to 10 GB and less than millisecond latency, which is almost in real-time (4G LTE takes 10–30 ms for round-trip communication). The 5G cellular network emerges as a new strong alternative to allow such connections, in a reliable, secure, and fast way, providing the IoV, as well as the V2X scenarios integration, where X could be vehicles, pedestrians, etc. [26]. It is expected that the 5G network can be able to attend the requirements for future IoV applications and to offer Intelligent Transport Systems (ITS) in several scenarios involving high mobility, dynamic network topology, and high data volume [27].

The 5G can connect more devices to the Internet without the interference that can occur with 4G since it uses different frequencies of the radio spectrum. Moreover, 5G offers enough bandwidth for connected vehicles to communicate. Compared to 4G, 5G significantly increases uplink and downlink sustainable bandwidth (the maximum bandwidth of the downlink will be around 20 Gbps and the maximum bandwidth of the uplink can be in the order of 100 Mbps). Autonomous vehicles (driverless vehicles) are merely one of the technologies that will be unlocked by 5G. The need for 5G technology will be further increased with autonomous vehicles. The low latency of the 5G and the efficiency of internet throughput are vital features for safety in autonomous vehicles.

3 IoV enabling technologies

In designing IoV architectures, it is paramount to consider a number of key enabling technologies and characteristics, including mobility, real-time processing, dynamic nature, context awareness, security, etc. In the following, we define the most important IoV technologies that will be considered as comparable criteria between literature architectures.

3.1 Software defined networking

Software-defined networking (SDN) as an emerging networking paradigm, is one of the most popular research fields in the IT industry [28]. SDN is a network architecture that centralizes and facilitates network management by the abstraction of functionalities. The SDN architecture is illustrated in Fig. 2. A key aspect of SDN is the decoupling of the control plane and the data plane. A unified interface to configure network equipment makes a large-scale customizable network possible and accelerates new service deployment in IoV [29]. The control plane is responsible for providing the policy rules and makes the packet transmission decisions. The data plane transmits the requests to the control plane and processes the packet transmission decisions. The SDN controller is considered a logically centralized control center. In addition to its role of data plane control and the deduction of the actions to exercise, the controller is in charge of the load balancing. Thus, the network functions of Roadside units (RSUs) and Base Stations (BSs) of the IoV will be virtualized and controlled centrally. SDN serves to simplify the

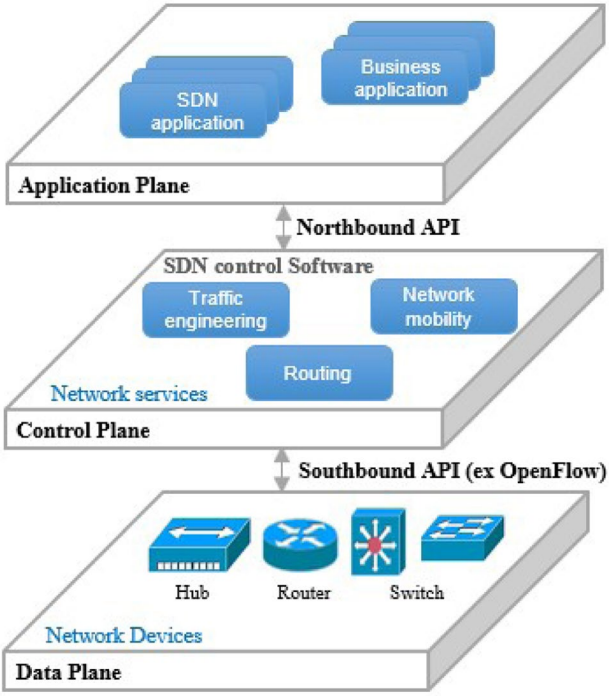

Fig. 2 SDN Architecture: SDN Applications communicate their network requirements to the SDN Controller via a Northbound API. The SDN Control software receives requirements from the Application Plane and relays them to the networking components. It also extracts information about the network from the Network devices via a Southbound API and communicates back to the SDN Applications. The Network devices, control the forwarding and data processing capabilities of the network

complexity of the network and offers a unique view of the devices and their protocols through the virtualization of the control layer. This can help solve many problems in traditional vehicular networks, including dynamic topology, network heterogeneity, and configuration. This also helps to foster the efficiency of V2V and V2I communications. Recently, several works [16, 30–32] addressed the SDN-based VANETs issue and considered it as an alternative to solve the problems encountered in conventional VANET networks to increase the quality of service (QoS) and save hardware costs.SDN is based on a standardized protocol in charge of the configuration commands and communication between the data plane and the control plane, thus simplifying the operations of the network system. There are several protocols such as Netconf, LISP, Open Flow, etc. The OpenFlow proposed by McKeown et al. in [33] is the most used typical protocol. This protocol allows the SDN controller to manage (add, modify, delete) rules of the flow table, thus facilitating the automatic configuration of the network.

In [34] the authors present a study on scheduling for cooperative data dissemination in a hybrid I2V and V2V communication environment. The proposed model and solution represents a VANET implementation of SDN concept. First, all the vehicles turn into V2V mode, find their neighbors and informs the RSU the list of its current neighboring vehicles (Vehicle-to-Roadside (V2R) mode). The RSU then selects sender and

receiver vehicles and corresponding data for V2V communication. Depending on its decision, each vehicle stays in either V2R or V2V mode to complete data transmission.

3.2 Cloud computing

Basically, the Cloud Computing has been defined in [35] as an infrastructure in which IT services (computing power, storage, databases, network management, software, analysis tools, etc.) are managed via the Internet by remote servers to which users connect. As one of the most significant improvements in modern data storage and computation technologies, cloud computing provides a powerful platform to perform complex and large scale computing [6]. Due to its rich set of infrastructures, storage, and computation services, Cloud computing provides an interesting environment for scientific experiments, data analysis and research [36].

Cloud computing has been one of the key technologies in the IoV [16]. The advancement in smart vehicles and information technologies motivate researchers and industries to pay attention to the combination of vehicular network with cloud computing in recent [37]. Cloud computing provides the idea of boundless storage, compute or network resources in the form of IaaS, PaaS and SaaS, which are extended to the inter-networked cars and infrastructure provided by VANETs [38]. In [39] the Cloud layer components allows collecting these results, storing them in a Big Data database for a high-level analysis and provide real-time visualization of the traffic situation. A cloud-based mutual authentication protocol aiming at ensuring efficient privacy preserving in IoV system is proposed in [40]. The protocol enables people the efficiently and intelligently travel mode while protecting their privacy from divulging and prevents the malicious tracking from outside attackers due to the anonymity of tag.

3.3 Fog computing

Sending all the collected data to the cloud has a serious disadvantage, when the latency is critical. To support the needs of data-intensive applications, research e orts have been investigating how to better exploit capabilities of the whole network aiming to extend the cloud computing functionality its edge [6]. In fact, the concept of edge computing could be considered to solve some of the cloud computing critical problems [41]. Fog computing [42] is part of the edge computing technology concept just as Mobile Edge Computing [43] and cloudlet [44]. Fog Computing [Fig. 3] is a virtualized platform initiated by Cisco in 2012 [45] addressing the need to extend Cloud Computing to manage the growing number of sensors, IoT devices, and real-time low-latency applications.

Rather than exchanging data with remote servers in the cloud, Fog computing provides data, computing, storage, and network services, to end users, from devices that are closer than traditional Cloud Computing data centers. Compared to Cloud computing, this computing layer is highly distributed and introduces additional services to end-devices [46]. It offers new types of applications and services by extending the paradigm of cloud computing to the edge of the network. This enables the distribution of the data processing at the edge of the network, which provides faster responses to ITS application queries and saves the network resources [6, 47]. Fog Computing has been applied to IoV services and applications, wireless sensor networks, smart cities, and more. It has been introduced into the cloud-based architecture to satisfy low latency requirement since the cloud center servers are far from the vehicles, which make the latency extremely high [16].

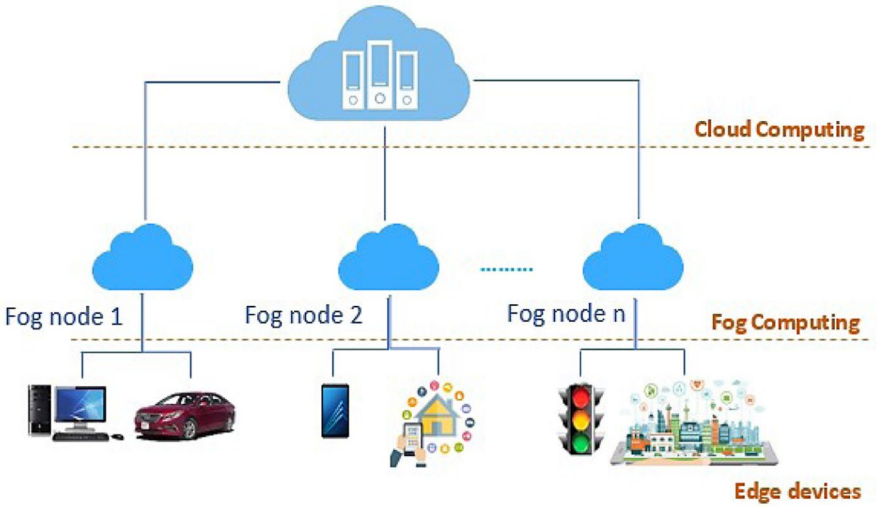

Fig. 3 Hierarchical structure of fog based system

In addition to the low latency, the fog computing layer is characterized by the use of wireless networks and mobile equipment, wide geographical distribution, and heterogeneity. These features make it an appropriate platform to provide services for connected vehicles such as data processing and real-time analysis and infotainment. The fog computing layer takes advantage of its proximity to the vehicle sensor layer and provides services that are extensions of the cloud layer such as Computing, Storage, and Network services [48]. In [48], the creation of several instances of Fog layer according to geographical distribution of connected objects is proposed. The fog computing architecture proposed in [14] is based on a publish/subscribe model where IoV knowledge is semantically represented, published and subscribed. A traffic congestion control scenario operating on top of the proposed architecture is presented as well. In a different approach, in [49] the authors proposed a vehicular fog computing (VFC) where they introduced the idea of exploiting vehicles as resource infrastructure for computation and communication.

3.4 Content-centric networking (CCN)

TCP-IP is a stateful connection that needs to be maintained if connected, therefore, IP address based connection is suffering from high mobility and extremely dynamic environment since high mobility will cause connection disruptions [29]. Information Centric Networks (ICN) is considered as a replacement of IP based network where the user does not care about the exact location of the source but the content itself. It is able to sustain packet delivery in unreliable and extreme environment, including the highly dynamic connectivity of mobile and ubiquitous computing [50]. These facts support Jacobson et al. Idea [50] of referring object with names as content centric on the network in place of IP. This has driven the ubiquitous to the new ICN paradigm: Content Centric Networking (CCN).

In CCN [54, 55], the user or an object can access data by name instead of an address, thus, the vehicles in the network do not need to be IP-addressable [56]. Unlike IP-based Internet architecture, which has many disadvantages such as reduced mobility and low

scalability, CCN architecture focuses on content rather than its source to convey the information to the interested parties.

In other words, it resolves the inquiry "what" and no longer, "where" which offers more flexibility. The study envisaged by Jacobson et al. in [57] allows users to broadcast and receive content from different devices and various networks and allows users to express their interests (the request from the content consumer). This serves to anticipate and deduce user needs and send only relevant information.

A deep learning-based CCN data dissemination approach for IoV was designed in [53] by taking into account the mobility of vehicles and types of content shared between vehicles. In this scheme, optimal V2V pairs are identified on the basis of trust, connection probability, energy available, and social score.

The authors in [55] propose an IP-based vehicular CCN framework, which focuses on acquiring contents related to a given position. When a requester acquires contents in the address-centric unicast way, the contents can be returned to the requester without depending on reverse paths. To reduce the content acquisition cost, contents in a given position are obtained from the nearest provider. The communication process proposed in [56] is shown in Fig. 4: the network layer of IoV based on CCN exchanges Interest and Data to communicate according to names. Vehicle A packs name into Interest and broadcasts it toward potential producers.

Using the Interest path in reverse, the Data will be returned to vehicle A when a middle node receives and has data matching the broadcasted interest. Otherwise, vehicle A needs to get a response from the server of CCN-IoV.

4 Candidate architectures for IoV

Several open and flexible architectural designs are recently proposed in the literature for IoV systems [4, 16, 29, 30, 58]. These architectures are divided mainly into two groups: architectures supporting emerging technologies like cloud computing, fog computing,

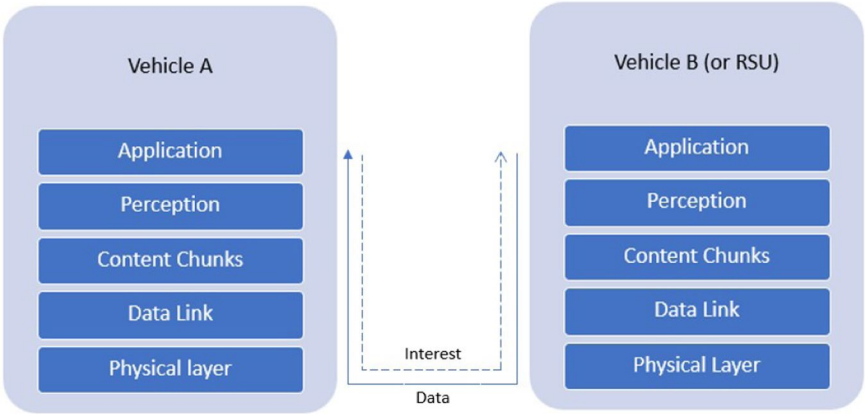

Fig. 4 The communication of CCN-IoV [56]: Vehicle A packs name into Interest and broadcasts it toward potential producers. The Data will be returned to vehicle A when a middle node has data matching the broadcasted interest

mobile edge computing, SDN, etc., and those which do not support these technologies. In this section, we examine and analyze different architectures by classifying them according to their number of layers.

4.1 Three-layered architecture

In a three-layered system, the bottom layer encompasses the physical structures (devices, access points, vehicles, sensors, on-board equipment (OBE), etc.). It communicates with the rest of the components to transmit the information collected during driving such as traffic conditions, location, vehicle condition, speed, etc. The middle layer is the one that enables communication and control of data flows. The top layer presents services and applications. In [58], the authors proposed a contextual architecture with mobile cloud support, divided into three layers according to the hierarchical spatial regions: vehicle, location, and cloud. Road Side Equipment (RSE) (at location calculation layer) and the neighboring OBE (at vehicle Layer) are interconnected and share contextual traffic information and entertainment resources. The latter consist of a network of vehicles and infrastructures that can generate accurate real-time traffic information.

From a network perspective, Nanjie [59] considered an IoV system as a three-tier system namely Client, Connection and Cloud. The client layer represents a communication terminal offering intra-vehicular and inter-vehicular communication and brings together the intelligence of the vehicle. The connection layer addresses the V2V, V2R, V2P and V2I interconnects for communication between VANETs and other heterogeneous networks. Cloud-based features such as virtualization, authentication, real-time interaction, and storage are handled by the cloud layer.

In [29], the physical layer includes vehicles communicating with the server, the access points that allow this communication, and the roadside devices (surveillance cameras, etc.). This layer collects the road conditions and sends data to servers or vehicles, switches, and servers that provide vehicle information services. The control layer is based on OpenFlow, which controls all data flows in the IoV. The controller handles the installation of OpenFlow rules in particular switches from application policies (path selection or access control). The strategy of each application is defined in the application layer. These strategies indicate how to provide services to vehicles (query service, location service and information about routes, etc.).

In [39] Nahri et al. introduce an architecture based on three layers: IoV, Fog Computing, and Cloud Computing. For the purpose of collecting and processing real-time events generated by vehicles and visualizing the traffic status on each section of road, they focused on the Fog Computing Layer. This layer is responsible for collecting and processing the massive event flows periodically generated at the IoV layer and for making these results available to the Cloud Computing layer.

In order to simplify the functionality of various components and to provide fewer control stations, the architecture presented in [60] follows a three-layered approach that separate planes for client, connection, and cloud layers. Intravehicular and intervehicular communications are handled by the client layer. It is as well responsible for enabling IoV addressing and maintaining a trustworthy identity in cyberspace. The connection layer processes the interconnectivity of various network components within a network and the integration of other available networks within a vehicular environment. The cloud layer enables the IoV services and applications and offers several cloud-based services such as mass

Table 2 Summary of the three-layered iov architectures

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/ Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (−) Drawbacks
Nahri et al. [39]	(1) IoV (2) Fog (3) Cloud	V2I, V2V	No	No	Both	No	No	None	Yes	(+) Collecting and analyzing events generated in real time (+) Visualizing real time traffic state on each road section (−) No consideration for the Big data processing requirements (−) Security issue has not been considered
Wang et al. [29]	(1) Physical (2) Control (3) Application	V2I, V2V, V2S V2P, V2R	No	Yes	Cloud	No	Yes	Control layer	Yes	(+) Reducing the number of rules without degrading the performance of data transmissions for real-time query services (−) Workload between the layers is not balanced (−) Latency of task processing is important

Table 2 (continued)

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/ Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (−) Drawbacks
Nanjie [59]	(1) Client (2) Connection (3) Cloud	V2V, V2R V2P, V2I	No	No	Cloud	No	No	Security as a service	No	(+) Ensuring real-time network ubiquity in terms of functionality and performance (-) Complexity of each layer
Wan et al. [56]	(1) Vehicle (2) Location (3) Cloud	V2V, V2R	No	No	Cloud	Yes	No	Cross layered	Yes	(+) Improving QoS (−) Connectivity, latency, and bandwidth
Sherazi et al. [58]	(1) Client (2) Connection (3) Cloud	V2I	No	No	Cloud	No	No	None	No	(+) Suitability coping with different types of applications against individual wireless technologies (−) Security and Big data have not been considered

storage, virtualization, and real-time interactions among different network entities. These aforementioned architectures are summarized in Table 2.

4.2 Four-layered architecture

In [61], the authors suggest a functional architecture that integrates the key technologies for the realization of IoV in a single platform. A bidirectional security authentication framework has been introduced to encapsulate the dedicated short-range communication protocol (DSRC), on-board unit and road-side unit technologies, integrated object logic and internet-based information infrastructure. The functional architecture has been divided into four layers:

- First layer (bottom): the detection layer composed of intermediate components and core components,
- Second layer: the network layer,
- Third layer: the data layer for data processing
- Fourth (top) layer: the application layer, which includes all functional application software (traffic information publication and vehicle owner service, etc.)

In addition, in this work, a system security architecture has been proposed. It implies that the data between RSU and OBU must be encrypted. RSU must provide the correct credentials to access a specific OBU. In [16], He et al. propose a four-layered architecture, integrating the fog computing and SDN to the IoV. In fact, fog computing could significantly reduce latency and enable mobility support and localization awareness. Moreover, the SDN provides the network with flexible centralized control. The infrastructure layer consists of vehicles with OBUs including processing units, sensors, location systems and radio transceivers. The fog computing layer consists of BS and RSU with computing and storage capabilities. This allows to obtain data and service required from cloud servers, status information traffic and store the relevant information transmitted. They also run the OpenFlow protocol to communicate with existing SDN controllers in the SDN control layer. These controllers handle cloud/fog network control centrally through the OpenFlow protocol. Storage and analysis of huge amounts of data collected from the devices are handled at the cloud computing layer through server clusters. To reduce the latency of task processing, the authors proposed an SDN-based modified constrained optimization particle swarm optimization (MPSO-CO) centralized load balancing algorithm. It allows the balancing of the workload between the cloud/fog devices. This has been proved by the results of numerical simulations. In addition, this algorithm improves the quality of service (QoS) in the proposed architecture.

In [62], a new layer coordination computing control layer is separated from the application layer. It is deployed to solve coordination and control computer problems such as data processing, resource allocation and computer swarm. This article constructs a Virtual Vehicle (VV), which represents an integrated image of the driver and vehicle in cyberspace and describes the nature and the architecture of a VV.

CISCO [42] has proposed an IoV architecture based on four layers, namely the end points layer, the infrastructure layer, the operation layer, and the service layer to enable the Vehicle-to-Business (V2B) communication. The first layer includes vehicles, software and V2V communication via 802.11p protocol. The technologies allowing the connection between all IoV actors (Wi-Fi Hotspots, 802.11u, 3G/4G, etc.) are defined at the

level of the infrastructure layer. The operation layer monitors policy enforcement and ow-based management. The last layer handles different types of cloud (public cloud, private cloud and enterprise cloud) and the services they offer to drivers. Liu et al. [63] envisaged a four-layered architecture, slightly different from the above-mentioned architectures. Comprising the application layer, the control layer, the virtualization layer, and the data layer and integrating both the SDN and fog computing paradigms, the proposed work enables logically centralized control via the separation of the control plane and the data plane. In the control layer of the hierarchical architecture, the SDN controller resides in the backbone network, which connects to cloud data centers and the Internet via the core network. The virtualization layer is responsible for the abstraction of networking, computation, communication, and storage resources in IoV. It also allow the service scheduling at the controller. The data layer consists of nodes with heterogeneous wireless communication interfaces such as LTE base stations, RSUs, WiFi access points (APs), 5G small cells, and vehicles. Among these nodes, a huge amount of data is generated, sensed, and shared.

The work by Ji et al. [9] also proposed a four-layered architecture. It consists of a Security Authentication layer that ensures the legitimacy of a vehicle and an RSU, a Data Acquisition layer that collects, classifies various types of data, and ensures that it is safely transmitted to the edge layer, an Edge layer that performs preliminary filtering, publishes data analysis results for local traffic events, and formulates a local decision-making scheme, a Cloud Platform layer in which the analysis of the collected traffic data and other tasks such as connection management, path planning, intelligent navigation, etc., are handled. The main features characterizing these architectures are shown in Table 3.

4.3 Five-layered architecture

In [56], the authors propose an IoV architecture based on Content-Centric Networking, divided into five parts: physical layer, data link layer, network layer, perception layer and application layer. The network layer is the neural center and the brain of the IoV, it uses fragments of CCN content to transmit and manage the information collected from the perception layer. A vehicle communicates its interest to potential producers. When an intermediate node of the road receives interest from this vehicle, it sends the corresponding data to the vehicle using the path of interest in the opposite direction. This data will be cached in the nodes to be able to respond to the following interests that require the same data.

Jiacheng et al. highlights in [30] the concept of SD-IoV (Software Defined IoV) that improves resource utilization, quality of service and network optimization in harsh vehicle network environments. The control plane provides APIs to perform the services hosted by the application plane and translate them into rules. Both the application plane and the control plane reside in cloud data centers and localized servers. The Upper Data Plane matches the switches and SDN-enabled wireless access infrastructures. The lower data plane includes the end users, which are the SDN compliant vehicles. Finally, the Knowledge layer represents an abstraction of the network state feedback functionalities.

The optimization of the number of layers and the improvement of the differentiability between the layers in Kaiwartya et al. [10] are the main priorities of the design of the five-layered architecture. In addition, a protocol stack has been designed with three layers: management, operation, and security to organize existing protocols based on architecture. The key features of the Five-Layered architectures are listed in Table 4.

Table 3 summary of the four-layered iov architectures

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/ Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (−) Drawbacks
Yang et al. [62]	(1) Vehicle network environment sensing and control (2) Network access and transport (3) Coordination computing control (4) Application	V2V, V2I	No	No	No	No	No	Not specified	No	(+) Solving the coordinative computing and control problems (−) No consideration for security
Li et al. [61]	(1) Sensing (2) Network (3) Data (4) Application	V2V, V2I	No	No	No	No	No	Bidirectional security authentication framework	Yes	(+) Encapsulating DSRC protocol, sensor technologies embedded object logic, and Internet-based information infrastructure (−) No real-time monitoring for the traffic flow
Bonomi [42]	(1) Services (2) Operation (3) Infrastructure (4) End points	V2V, V2I	No	No	Yes	No	No	Cross layered	No	(+) Facilitating commercial business services integration with vehicles (−) Transmitting collected data without preprocessing

Table 3 (continued)

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/ Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (−) Drawbacks
He et al. [16]	(1) Cloud computing (2) SDN control (3) Fog computing (4) Infrastructure	V2V, V2I	No	Yes	Yes	No	No	Not specified	Yes	(+) Decreasing the latency (+) Improving the QoS (−) Only latency was considered as an aspect of QoS
Kai Liu et al. [63]	(1) Data layer (2) Virtualization (3) Control (4) Application	I2V, V2V	No	Yes	Both	No	Yes	Not specified	No	(+) Improving the scalability and reliability of information services while increasing the flexibility of application management (−) Absence of interconnection with heterogeneous networks and other communication devices. (−) No consideration for security

Table 3 (continued)

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/ Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (−) Drawbacks
Ji et al. [9]	(1) Cloud Platform (2) Edge (3) Data Acquisition (4) Security Authentication	V2V, V2I, V2R, V2P	No	No	Cloud	No	No	Security Authentication layer	No	(+) Ensuring the legitimacy of the vehicle requesting to connect to the network (+) Including an Edge layer that performs filtering and analysis on the collected data and publishes data analysis results in real time (−) No consideration for Big data

4.4 Seven-layered architecture

Even though the number seems high, researchers admit that increasing the number of layers can be beneficial for seamless interconnection of all components in an IoV environment. In [4], the authors propose a seven-layer architecture. The defining features of this architecture are summarized in Table 5. The bottom layer focuses on the direct interaction with the driver and serves to reduce his distractions through a management interface. The data acquisition layer deals with the collection of data from internal and external sensors, traffic lights, inter-vehicular communications, etc.

The analysis of this information is the role of the data filtering and pre-processing layer. Based on selection parameters (congestion, and quality of service level in the different available networks, privacy and security, etc.), the communication layer selects the best network to send the information. The responsible layer for managing service providers is the control and management layer. A processing layer is provided to handle large amounts of information using cloud computing infrastructures locally and remotely. Security functions (authentication, integrity, non-repudiation and confidentiality, access control, availability, etc.) are handled by the last (top) layer that communicates directly with the rest of the layers.

Another group of researchers [64] proposed a seven-layered IoV model architecture, namely vehicle identification layer, object layer, inter-intra devices layer, communication layer, cloud services layer, big data and multimedia computation layer, and application layer. The main role of the Identification layer is to detect vehicles and non-vehicle devices. The physical objects layer gathers all the data of all objects (vehicle and non-vehicle) and transmits the collected data to the intra-inter devices layer for further processing. The intra-inter devices layer together with the communication layer enables the system to support all types of interaction models including V2V, V2R, V2I, V2B, V2H, V2X, V2G, V2P, V2D, V2S, and D2D interactions and connect the different and heterogeneous objects and networks. The cloud service layer provides infrastructure, hardware, computing platforms, as well as software services for IoV systems. The Multimedia and Big data layer consists of three sublayers responsible for data pre-processing, Big data computation and analytics, and intelligent transportation. Smart applications and services such as traffic safety and efficiency, multimedia-based infotainment, traffic signal control systems, container management systems, etc., are covered by the Application layer.

5 Discussion

The architecture issue is one of the core issues associated with the design and development of an IoV system. Consequently, it is important to select the proper technologies and provide the security that an IoV system requires. Balancing the workload between layers to reduce the process complexity and provide a transparent view, can also improve the QoS. In Tables 2, 3, 4 and 5 we present a comparison of various architectures and carry out a brief critical overview in this section. The comparison was conducted according to a number of criteria such as the number of layers, the employed technologies and security. In these tables, we expose the advantages and disadvantages of each mentioned architecture.

In [27], a global view of the network and high scalability were proposed by separating the data plane from the control plane, which gives different views for each layer and

Table 4 Summary of the five-layered iov architecture

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (−) Drawbacks
Li et al. [56]	(1) Physical (2) Data link (3) Network Perception Application	V2V, V2R	Yes	No	No	No	No	Not specified	Yes	(+) Improving mobile communication performance of IoV (−) No decoupling of control plane and data plane (−) No consideration for security
Kaiwartya et al. [10]	(1) Perception (2) Coordination (3) Artificial intelligence (4) Application (5) Business	V2I, V2V V2S, V2P, V2R	No	No	No	No	No	Security plane	No	(+) Optimizing the number of layers and enhancing the differentiability among layers (−) No notification management (−) Transmitting collected data without preprocessing
Jiacheng et al. [30]	(1) Lower Data plane (2) Upper Data plane (3) Control plane Application plane knowledge plane	V2V, V2I	No	Yes	No	No	No	Not specified	No	(+) Improving resource utilization, service quality, and network optimization (−) a full functional layered architecture is not discussed

simplifies their tasks. Thanks to the SDIV architecture, the real-time query service in IoV is developed. A similar service assimilated to a high-level analysis of events and real-time visualization of the traffic situation is proposed by Nahri et al. [39], which offers better traceability. Similar to [27], the work in [63] integrated the paradigms of SDN to separate the data plane from the control plane to best exploit their synergistic effects on information services in IoV. Besides, the SDN controller present in the control layer has access to a uniform view of virtual resources based on the abstraction of resources at the virtualization layer. This could facilitate service scheduling instead of directly managing heterogeneous physical resources, facilitate adaptive resource allocation and QoS oriented services.

The IoV architecture illustrated in [44] allows vehicles and drivers to access a broad range of service providers, and to promote the integration of commercial business services with vehicles. Likewise, in the architecture proposed by [60], enabling all the IoV services and applications is handled by the cloud layer. A broad range of cloudbased services, such as mass storage, virtualization and real-time interactions between different network entities are provided. Some potential commonalities are shared in [58] and [59] such as the functionality of certain layers and the services offered by the cloud.

The architecture model in [10] considers the concept of heterogeneous networks in the IoV by processing the different structure of information received from heterogeneous networks by the Artificial intelligence layer. The same concept has been considered by L. Minn et al. [64] by integrating and connecting heterogeneous network objects, including multimedia devices, to provide specific services. This was established through the combination of the Inter-Intra Devices Layer and the Communication Layer.

On the other hand, this architecture addressed the problem of processing and analyzing Big Data, whereas most of the proposed architectures do not meet the requirements of processing and analyzing Big Data in real time, which can lead to serious issues. Big data processing and analysis was considered as smart heterogeneous multimedia objects that can interact and cooperate with each other and with other internet-connected things to facilitate the multimedia services and applications. The Big data computation layers were designed to take into account, process, and analyze Big data, multimedia data, along with other sophisticated objects. The third layer of the architecture in [10] responsible for the storage, processing and analysis of information received from the lower layer has two major operational components, namely Vehicular Cloud and Big analytics Data which enables the processing and analysis of Big Data in real time.

As a crucial role in the design and deployment of IoV systems, a few works focused on the security and privacy issues. In [58], the security and privacy issues are reflected in different layers, however in [62] authentication is offered as a service through the cloud. An effective communication process through the discussion of interest is as well proposed in [59]. It should be noted that this architecture is capable of supporting network caching and multicasting without additional protocols or mechanisms. Whereas authors in [10] consider that security protocols for IoV as an open research challenge due to the unavailability of clear definitions of layer wise security protocols, they put forward some protocols that may be employed in their architecture such as IEEE 1609.2, Security Information Connector (S-IC), Security Management Information Base (S-MIB) and Hardware Security Module (HSM). The security issue in [9] was considered in the security authentication layer, which aims to ensure the legitimacy of the identity of the vehicle and the RSU requesting to connect to the network. With the help of a unique factory serial number assigned to a legal vehicle or RSU, the falsification of legitimate vehicle's or RSU's data from an illegal vehicle or an illegally installed RSU could be revealed. The consideration of security (authentication, authorization, etc.) must be paramount, which is not the case for some architectures

Table 5 Summary of the seven-layered IoV architecture

IoV architectures	Name of layers	Communication links models	CCN control	SDN control	Cloud/Fog	Context awareness	Case study	Security	Experiment	(+) Advantages (-) Drawbacks
Contreras-Castillo et al. [4]	(1) Vehicle interface (2) Data acquisition (3) Data filtering and preprocessing (4) Communication (5) Control and management (6) Processing (7) Security	V2V, V2I, V2P, V2S, V2R, V2D, Roadside-to-Roadside, Roadside to Personal device, Sensor to Actuator	No	No	No	No	No	Security layer	No	(+) Providing a seamless integration (+) Interconnection of all the network components (+) Dissemination of data into an IoV environment (−) No real-time analysis of large amount of information
Li-minn et al. [64]	(1) Identification (2) Physical objects (3) Inter-intra devices (4) Communication (5) Cloud services (6) Multimedia and big data computation (7) Application	V2V, V2R, V2X, V2G, V2S, V2I, V2B, V2H, V2P, V2D, D2D interactions	No	No	Cloud	No	No	Cross layered	Yes	(+) Multimedia and Big data computation (+) Connection of different heterogeneous objects and netwoks due to the intra-inter devices layer and the communication layer (−) No consideration for QoS

[16, 30, 39, 56, 62]. As balancing high security along with good performance, ensuring security, and preventing privacy breaches remain a major challenge [7], the application requirement for real-time responses becomes an enhanced need. In this context, in [41] authors extracted real time traffic situation in each road network section and analyzed the events generated by connected vehicles in real-time.

Some researchers believe that increasing the number of layers provides more seamlessness and reduces the processing complexity of each layer. Nonetheless, the greater is the number of communicating agents in the IoV, the more there will be a network overhead in addition to increased latency. Even though the proposed architecture in [4], allows seamless and transparent interconnection of all network components and data dissemination in an IoV environment, however, data processing using the cloud may take a long time. Therefore, a real-time analysis of large amounts of information seems to be impossible. In this context, the work introduced by Li-Minn et al. [64] has developed seven main elements in the Universal IoV architecture and seven corresponding core layers.

Despite the fact that the proposed architecture considered a new layer enabling the integration and cooperation among heterogeneous objects and networks, including multimedia devices, none of the QoS aspect, such as efficiency, flexibility, performance, and latency was taken into consideration, whereas some authors have focused on the QoS as a crucial feature of deploying an IoV architecture. Based on this, the architecture of Liu et al. [63] for IoV aimed to enhance the scalability and reliability of information services and improve agility and flexibility of application management. Similarly, selection parameters, in particular, QoS level over the different available networks, information relevance, privacy and security among others, were taken into consideration in [64] by the communication layer, which aims to select the most suitable network to send the information. The authors in [9] believe their network architecture is designed with lower latency, greater data throughput, higher security, and massive connectivity. In the SDCFN architecture proposed in [16], the simulation results indicate that the SDN-based architecture could effectively decrease the latency and enhances the QoS, which could apply to the IoV to process latency-sensitive tasks more efficiently.

Several previously mentioned architectures are convenient for supporting various types of IoV applications with high QoS requirements as they perform a large number of computations in limited time due to the deployed technologies such as cloud computing, fog computing, SDN, etc., capable to realize such computation offloading.

We believe that this study illustrates the importance of the architectural design, addresses new challenges to computation and storage resources management, security, deployment, etc., and can build a solid base not only to design a satisfactory architecture for IoV but also an unavoidable step towards a more appropriate future in which issues such as the huge amounts of data generated by vehicles, resources management, and a lot of others would be encountered.

6 Conclusion

IoV systems have emerged as part of Intelligent Transportation Systems to provide additional Internet connectivity functionalities to traditional VANETs. This emerging concept poses several challenges that need to be addressed such as security, routing, scalability, mobility, etc. Architectural design is considered as one of the most important challenges of IoV systems. In this paper, we have presented a comparative study of several IoV

architectures proposed in the literature. We classified these architectures according to the number of layers and compared them according to several criteria such as security, supported communication models, deployed technologies, etc. This survey work consists of an exhaustive study of existing IoV architectures. It is intended to provide a base of analysis for future works dealing with architecture design improvement.

References

1. Atzori L, Lera A, Morabito G (2014) From "smart objects" to "social objects": The next evolutionary step of the internet of things. IEEE Commun Mag 52(1):97–105
2. Fortino G, Trun OP (eds) (2014) Internet of things based on smart objects: Technology, middleware and applications. Springer, Berlin
3. Wan J, Liu J, Shao Z, Vasilakos A, Imran M, Zhou K (2016) Mobile crowd sensing for tra c prediction in internet of vehicles. Sensors 16:88
4. Contreras-Castillo J, Zeadally S, Guerrero-Ibanez JA (2018) Internet of vehicles: Architecture, protocols, and security. IEEE Internet Things J 5(5):3701–3709
5. Borcoci E, Obreja S,Vochin, M. (2017) Internet of vehicles functional architectures comparative critical study. In: The 9th international conference on advances in future internet, AFIN, pp 10–14.
6. Darwish TS, Bakar KA (2018) Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues. IEEE Access 6:15679–15701
7. Sharma S, Kaushik B (2019) A survey on internet of vehicles: applications, security issues and solutions. VehicCommun 100182:1. https://doi.org/10.1016/j.vehcom.2019.100182
8. Shen X, Fantacci R, Chen S (2020) Internet of Vehicles [Scanning the Issue]. Proc IEEE 108(2):2
9. Ji B, Zhang X, Mumtaz S, Han C, Li C, Wen H, Wang D (2020) Survey on the internet of vehicles: network architectures and applications. IEEE Commun Stand Mag 4(1):34–41. https://doi.org/10.1109/mcomstd.001.1900053
10. Kaiwartya O, Abdullah AH, Cao Y, Altameem A, Prasad M, Lin CT, Liu X (2016) Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects. IEEE Access 4:5356–5373
11. Lee EK, Gerla M, Pau G, Lee U, Lim JH (2016) Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. Int J DistribSensNetw 12(9):1
12. Gross M (2016). A planet with two billion cars. http://www.sciencedirect.com/science/article/pii/S0960982216303414. Accessed 16 Dec 2018.
13. Huang T (2014) Surveillance video: The biggest big data. Computing Now 7(2):82–91
14. Chun S, Shin S, Seo S, Eom S, Jung J, Lee KH (2016) A pub/sub- based fog computing architecture for Internet-of-Vehicles. In: IEEE international conference on cloud computing technology and science (CloudCom). IEEE, pp 90–93
15. Nitti M, Girau R, Floris A, Atzori L (2014). On adding the social dimension to the internet of vehicles: Friendship and middleware. In: IEEE international black sea conference on communications and networking (BlackSeaCom). IEEE, pp 134–138
16. He X, Ren Z, Shi C, Fang J (2016) A novel load balancing strategy of softwaredened cloud/fog networking in the Internet of Vehicles. China Commun 13(2):140–149
17. Gartner (2015) Gartner says by 2020, a quarter billion connected vehicles will enable new in-vehicle services and automated driving capabilities. Gartner. https://www.gartner.com/en/newsroom/press-releases/2015-01-26-gartner-says-by-2020a-quarter-billion-connected-vehicleswill-enable-new-in-vehicle-services-and-automateddrivingcapabilities. Accessed 21 January 2019.
18. Lim J, Jeong YS, Park D-S, Lee H (2016) An efficient distributed mutual exclusion algorithm for intersection trac control. J Supercomput 74(3):1090–1107. https://doi.org/10.1007/s11227-016-1799-3
19. National Highway Trac Safety Administration (2014) Fact sheet: improving safety and mobility through connected vehicle technology
20. Feukeu EA, Djouani K, Kurien A (2015) Performance evaluation of the ADSA in a vehicular network: MAC approach in IEEE 802.11 p. J Ambient Intell Hum Comput 6(3):351–360
21. Hoymann C, Astely D, Stattin M, Wikstrom G, Cheng JF, Hoglund A et al (2016) LTE release 14 outlook. IEEE Commun Mag 54(6):44–49
22. Tseng YL (2015) LTE-advanced enhancement for vehicular communication. IEEE WirelCommun 22(6):4–7

23. Buehler R, Pucher J (2017) Trends in walking and cycling safety: recent evidence from high-income countries, with a focus on the United States and Germany. 107(2):281–287
24. Litman T, Blair R (2017). Managing personal mobility devices (PMDs) on nonmotorized facilities. Victoria Transport Policy Institute
25. Cai H, Xu B, Jiang L, Vasilakos AV (2017) IoT-based big data storage systems in cloud computing: perspectives and challenges. IEEE Internet Things J 4(1):75–87
26. Storck CR, Duarte-Figueiredo F (2019) A 5G V2X ecosystem providing internet of vehicles. Sensors 19(3):550
27. Ge X, Li Z, Li S (2017) 5G software defined vehicular networks. IEEE Commun Mag 55(7):87–93
28. Stojmenovic I (2014). Fog computing: a cloud to the ground support for smart things and machine-to-machine networks. In: Australasian telecommunication networks and applications conference (ATNAC). IEEE, pp 117–122
29. Wang M, Wu J, Li G, Li J, Li Q, Wang S (2017). Toward mobility support for informationcentric IoV in smart city using fog computing. In: IEEE international conference on smart energy grid engineering (SEGE). IEEE, pp 357–361
30. Jiacheng C, Haibo ZHOU, Ning Z, Peng Y, Lin G, Xuemin S (2016) Software defined Internet of vehicles: architecture, challenges and solutions. J CommunInf Networks 1(1):14–26
31. Wang X, Wang C, Zhang J, Zhou M, Jiang C (2017) Improved rule installation for realtime query service in software-de ned internet of vehicles. IEEE Trans IntellTranspSyst 18(2):225–235
32. Ji X, Yu H, Fan G, Fu W (2016) SDGR: an SDN-based geographic routing protocol for VANET. In: 2016 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE, pp 276–281
33. McKeownN AT, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Turner J (2008) OpenFlow: enabling innovation in campus networks. ACM SIGCOMM ComputCommun Rev 38(2):69–74
34. Liu K, Ng JK, Lee V, Son SH, Stojmenovic I (2016) Cooperative data scheduling in hybrid vehicular ad hoc networks: VANET as a software defined network. IEEE/ACM Trans Netw (TON) 24(3):1759–1773
35. Mell P, Grance T (2011) The NIST definition of cloud computing
36. Gunarathne T, Zhang B, Wu TL, Qiu J (2013) Scalable parallel computing on clouds using Twister4Azure iterative MapReduce. Fut Gen ComputSyst 29(4):1035–1048
37. Park Y, Sur C, Rhee KH (2015) Pseudonymous authentication for secure V2I services in cloud-based vehicular networks. J Ambient Intell Hum Comput 7(5):661–671. https://doi.org/10.1007/s12652-015-0309-4
38. Gupta M, Sandhu R. (2018). Authorization framework for secure cloud assisted connected cars and vehicular internet of things. In: Proceedings of the 23nd ACM on symposium on access control models and technologies. ACM, 2018. pp. 193–204.
39. Nahri M, Boulmakoul A, Karim L, Lbath A (2018) IoV distributed architecture for realtimetrac data analytics. ProcediaComputSci 130:480–487
40. Fan K, Jiang W, Luo Q, Li H, Yang Y (2019). Cloud-based RFID Mutual Authentication Scheme for Efficient Privacy Preserving in IoV. J Frankl Inst
41. Masip-Bruin X, Marn-Tordera E, Tashakor G, Jukan A, Ren GJ (2016) Foggy clouds and cloudy fogs: a real need for coordinated management of fog-to-cloud computing systems. IEEE WirelCommun 23(5):120–128
42. Bonomi F, Milito R, Natarajan P, Zhu J (2014) Fog computing: A platform for internet of things and analytics. Big data and internet of things: A roadmap for smart environments. Springer, Cham, pp 169–186
43. Patel M, Naughton B, Chan C, Sprecher N, Abeta S, Neal A (2014) Mobile-edge computing introductory technical white paper. White Paper, Mobile-edge Computing (MEC) industry initiative, pp 1089–7801
44. Satyanarayanan M, Bahl P, Caceres R, Davies N (2009) The case for vm-based cloudlets in mobile computing. IEEE PervasComput 4:14–23
45. Bonomi F, Milito R, Zhu J, Addepalli S (2012) Fog computing and its role in the internet of things. In Proceedings of the first edition of the MCC workshop on Mobile cloud computing. ACM, pp. 13–16.
46. Yi S, Li C, Li Q (2015) A survey of fog computing: concepts, applications and issues. In Proceedings of the 2015 workshop on mobile big data. ACM, pp 37–42
47. Tang B, Chen Z, Hefferman G, Pei S, Wei T, He H, Yang Q (2017) Incorporating intelligence in fog computing for big data analysis in smart cities. IEEE Trans IndInf 13(5):2140–2150
48. Negash B, Rahmani AM, Liljeberg P, Jantsch A (2018) Fog computing fundamentals in the internet-of-things. Fog computing in the internet of things. Springer, Cham, pp 3–13

49. Hou X, Li Y, Chen M, Wu D, Jin D, Chen S (2016) Vehicular fog computing: a viewpoint of vehicles as the infrastructures. IEEE Trans VehTechnol 65(6):3860–3873
50. Jacobson V, Smetters DK, Thornton JD, Plass M, Briggs N, Braynard R (2009). Networking named content. In: Proceedings of the 5th international conference on emerging networking experiments and technologies, CoNEXT, ACM, New York, pp 1–12
51. Bari MF, Chowdhury SR, Ahmed R, Boutaba R, Mathieu B (2012) A survey of naming and routing in information-centric networks. IEEE Commun Mag 50(12):44–53
52. Ahlgren B, Dannewitz C, Imbrenda C, Kutscher D, Ohlman B (2012) A survey of information-centric networking. IEEE Commun Mag 50(7):26–36
53. Gulati A, Aujla GS, Chaudhary R, Kumar N, Obaidat M S (2018). Deep learning-based content centric data dissemination scheme for internet of vehicles. In: IEEE international conference on communications (ICC). IEEE, pp 1–6
54. Zhang L, Estrin D, Burke J, Jacobson V, Thornton JD, Smetters DK, Papadopoulos C (2010). Named data networking (ndn) project. Relat˙orio T˙ecnico NDN-0001, Xerox Palo Alto Research Center-PARC, pp 157–158.
55. Wang X, Wang X (2019) Vehicular content-centric networking framework. IEEE Syst J 13(1):519–529
56. Li Z, Chen Y, Liu D, Li X (2017) Performance analysis for an enhanced architecture of IoV via content-centric networking. EURASIP J WirelCommunNetw 2017(1):124
57. Jacobson V, Smetters DK, Thornton JD, Plass M, Briggs N, Braynard R (2009). Networking named content. In: Proceedings of the 5th international conference on emerging networking experiments and technologies, CoNEXT. ACM, New York, pp. 1 12.
58. Wan J, Zhang D, Zhao S, Yang L, Lloret J (2014) Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions. IEEE Commun Mag 52(8):106–113. https://doi.org/10.1109/mcom.2014.6871677
59. Nanjie L (2011). Internet of Vehicles your next connection. WinWin Magazine, Issue 11, HUAWEI. OAA. (2016). Open automotive alliance (OAA). Retrieved December 16, 2016, from http://www.openautoalliance.net/#about
60. Sherazi HHR, Khan ZA, Iqbal R, Rizwan S, Imran MA, Awan K (2019). A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication. Mobile Inf Syst
61. Li B, Li Y (2012) A bi-directional security authentication architecture for the internet of vehicles. Applied Mathematics and Information Sciences, Special Issues, pp 821–827
62. Yang F, Li J, Lei T, Wang S (2017) Architecture and key technologies for Internet of Vehicles: a survey. J CommunInf Networks 2(2):1–17
63. Liu K et al (2019) A hierarchical architecture for the future internet of vehicles. IEEE Commun Mag 57(7):41–47
64. L. Minn et al (2018) Deployment of IoV for smart cities: applications, architecture, and challenges. IEEE Access